bitdefender

antivirus 2010

Guide d'utilisation

Copyright© 2009 BitDefender

BitDefender Antivirus 2010
Guide d'utilisation

Publié le 2009.10.02

Copyright© 2009 BitDefender

Notice Légale

Tous droits réservés. Aucune partie de ce manuel ne peut être reproduite ou transmise, sous aucune forme et d'aucune façon, électronique ou physique, y compris photocopies, enregistrement, ou par quelque moyen de sauvegarde ou de restauration que ce soit, sans une autorisation écrite d'un représentant officiel de BitDefender. L'inclusion de courtes citations dans des textes n'est possible qu'avec la mention de la source. Le contenu ne peut en aucun cas être modifié.

Avertissement. Ce produit et sa documentation sont protégés par copyright. Les informations de ce document sont données « à titre indicatif », sans garantie. Bien que toutes les précautions aient été prises lors de la préparation de ce document, les auteurs ne pourront être tenus responsables envers quiconque de toute perte ou dommage occasionné, ou supposé occasionné, directement ou indirectement par les informations contenues dans ce document.

Ce manuel contient des liens vers des sites Web de tiers qui ne sont pas sous le contrôle de BITDEFENDER, et BITDEFENDER n'est pas responsable du contenu de ces sites. Si vous accédez à l'un des sites Web d'une tierce partie fourni dans ce document, vous le ferez à vos propres risques. BITDEFENDER indique ces liens uniquement à titre informatif, et l'inclusion de ce lien n'implique pas que BITDEFENDER assume ou accepte la responsabilité du contenu de ce site Web d'un tiers.

Marques commerciales. Des noms de marques peuvent apparaître dans ce manuel. Toutes les marques, enregistrées ou non, citées dans ce document, sont la propriété exclusive de leurs propriétaires respectifs.

Table des matières

Contrat de licence logiciel pour utilisateur final ix

Préface xiv
1. Conventions utilisées dans ce manuel xiv
1.1. Normes Typographiques xiv
1.2. Avertissements xv
2. Structure du manuel xv
3. Commentaires xvi

Installation et désinstallation 1

1. Configuration requise 2
1.1. Configuration système minimale 2
1.2. Configuration système recommandée 2
1.3. Logiciels pris en charge 2

2. Préparation de l'Installation 4
2.1. Installation de BitDefender sur un NetBook/Mini-PC 4

3. Installation de BitDefender 5
3.1. Assistant d'enregistrement 8
3.1.1. Étape 1 - Enregistrer BitDefender Antivirus 2010 9
3.1.2. Etape 2 - Création d'un compte BitDefender 10
3.2. Assistant de configuration 12
3.2.1. Étape 1 - Sélectionner le Profil d'Utilisation 13
3.2.2. Étape 2 - Description de l'ordinateur 14
3.2.3. Étape 3 - Sélectionner l'Interface Utilisateur 15
3.2.4. Étape 4 - Configurer le Réseau BitDefender 16
3.2.5. Étape 5 - Sélectionner les tâches à exécuter 17
3.2.6. Étape 6 - Fin 18

4. Mettre à niveau 20

5. Réparer ou supprimer BitDefender 21

Pour démarrer 22

6. Présentation 23
6.1. Ouverture de BitDefender 23
6.2. Modes d'affichage de l'interface utilisateur 23
6.2.1. Mode Débutant 24
6.2.2. Mode Intermédiaire 27
6.2.3. Mode Expert 28
6.3. Icône de la zone de notification 31
6.4. Barre de l'activité d'analyse 32
6.4.1. Analyser Fichiers et Dossiers 32
6.4.2. Désactiver/Restaurer la Barre d'Activité d'Analyse 33
6.5. Analyse Manuelle BitDefender 33
6.6. Mode Jeu et Mode Portable 34

6.6.1. Mode Jeu 35
6.6.2. Mode Portable 36
6.7. Détection automatique de périphérique 36
7. Correction des problèmes 38
7.1. Assistant de Correction des Problèmes 38
7.2. Configuration du système de contrôle 40
8. Configuration des Paramètres de base 42
8.1. Paramètres de l'Interface Utilisateur 43
8.2. Paramètres de sécurité 44
8.3. Paramètres généraux 46
9. Historique et Événements 48
10. Enregistrement et Mon compte 50
10.1. Enregistrement de BitDefender Antivirus 2010 50
10.2. Activation de BitDefender 51
10.3. Achat de clés de licence 54
10.4. Renouvellement de votre licence 54
11. Assistants 55
11.1. Assistant d'analyse antivirus 55
11.1.1. Étape 1 sur 3 - Analyse 55
11.1.2. Étape 2 sur 3 - Sélectionner des actions 57
11.1.3. Étape 3 sur 3 - Voir les résultats 58
11.2. Assistant d'Analyse Personnalisée 60
11.2.1. Etape 1 sur 6 – Fenêtre de Bienvenue 60
11.2.2. Étape 2/6 - Sélectionner la Cible 61
11.2.3. Étape 3/6 - Sélectionner les Actions 62
11.2.4. Étape 4/6 - Paramètres Supplémentaires 64
11.2.5. Étape 5/6 - Analyse 65
11.2.6. Étape 6/6 - Voir les résultats 66
11.3. Assistant du Contrôle de Vulnérabilité 67
11.3.1. Etape 1/6 - Sélectionnez les vulnérabilités à vérifier 68
11.3.2. Etape 2/6 - Vérifier les vulnérabilités 69
11.3.3. Étape 3/6 - Mettre à jour Windows 70
11.3.4. Étape 4/6 - Mettre à jour les applications 71
11.3.5. Étape 5/6 - Modifier les mots de passe vulnérables 72
11.3.6. Étape 6/6 - Voir les résultats 73
Mode Intermédiaire 74
12. État 75
13. Antivirus 77
13.1. Zone d'état 77
13.1.1. Configuration des paramètres de contrôle 78
13.2. Tâches rapides 79
13.2.1. Mettre à jour BitDefender 79
13.2.2. Analyser avec BitDefender 80

14. Antispyware 82
14.1. Zone d'état 82
14.2. Tâches rapides 83
14.2.1. Mettre à jour BitDefender 83
14.2.2. Analyser avec BitDefender 84
15. Vulnérabilité 86
15.1. Zone d'état 86
15.2. Tâches rapides 87
16. Réseau 88
16.1. Tâches rapides 88
16.1.1. Rejoindre le réseau BitDefender 89
16.1.2. Ajout d'ordinateurs au réseau BitDefender 89
16.1.3. Gestion du réseau BitDefender 91
16.1.4. Analyse de tous les ordinateurs 93
16.1.5. Mise à jour de tous les ordinateurs 94
16.1.6. Enregistrement de tous les ordinateurs 95
Mode Expert 96
17. Général 97
17.1. État 97
17.1.1. État global 98
17.1.2. Statistiques 100
17.1.3. Présentation 101
17.2. Configuration 102
17.2.1. Paramètres généraux 102
17.2.2. Paramètres du rapport antivirus 103
17.3. Informations système 104
18. Antivirus 106
18.1. Protection en temps réel 106
18.1.1. Configuration du niveau de protection 107
18.1.2. Personnaliser le niveau de protection 108
18.1.3. Configuration d'Active Virus Control 112
18.1.4. Désactivation de la protection en temps réel 115
18.1.5. Configurer la protection antiphishing 115
18.2. Analyse à la demande 117
18.2.1. Tâches d'analyse 118
18.2.2. Utilisation du menu de raccourcis 119
18.2.3. Création de tâches d'analyse 121
18.2.4. Configuration des tâches d'analyse 121
18.2.5. Analyse des fichiers et des dossiers 133
18.2.6. Afficher les journaux d'analyse 141
18.3. Objets exclus de l'analyse 142
18.3.1. Exclusion des chemins de l'analyse 144
18.3.2. Exclusion des extensions de l'analyse 147
18.4. Zone de quarantaine 151
18.4.1. Gérer les fichiers en quarantaine 152

18.4.2. Configuration des paramètres de la quarantaine ... 153
19. Contrôle vie privée ... 155
19.1. État du Contrôle Vie privée ... 155
19.1.1. Configuration du niveau de protection ... 156
19.2. Contrôle d'identité ... 156
19.2.1. Création de règles d'Identité ... 159
19.2.2. Définition des Exceptions ... 162
19.2.3. Gestion des règles ... 163
19.2.4. Règles Définies par d'Autres Administrateurs ... 164
19.3. Contrôle du registre ... 164
19.4. Contrôle des cookies ... 166
19.4.1. Fenêtre de configuration ... 168
19.5. Contrôle des scripts ... 170
19.5.1. Fenêtre de configuration ... 171
20. Vulnérabilité ... 173
20.1. État ... 173
20.1.1. Réparation des vulnérabilités ... 174
20.2. Configuration ... 174
21. Cryptage de messagerie instantanée ... 176
21.1. Désactiver le cryptage pour des utilisateurs spécifiques ... 177
22. Mode Jeu / Portable ... 179
22.1. Mode Jeu ... 179
22.1.1. Configuration du Mode Jeu automatique ... 180
22.1.2. Gestion de la liste de jeux ... 181
22.1.3. Configuration des paramètres du Mode Jeu ... 182
22.1.4. Changer le raccoruci clavier du Mode Jeu ... 183
22.2. Mode Portable ... 183
22.2.1. Configuration des paramètres du Mode Portable ... 184
23. Réseau Domestique ... 185
23.1. Rejoindre le réseau BitDefender ... 185
23.2. Ajout d'ordinateurs au réseau BitDefender ... 186
23.3. Gestion du réseau BitDefender ... 188
24. Mise à jour ... 191
24.1. Mise à jour automatique ... 191
24.1.1. Demandes de mise à jour ... 192
24.1.2. Désactiver la mise à jour automatique ... 193
24.2. Paramètres de mise à jour ... 193
24.2.1. Paramétrage des emplacements de mise à jour ... 194
24.2.2. Configuration de la mise à jour automatique ... 195
24.2.3. Configuration de la mise à jour manuelle ... 195
24.2.4. Configuration des paramètres avancés ... 196
24.2.5. Gestion des serveurs proxy ... 196
25. Enregistrement ... 199
25.1. Enregistrement de BitDefender Antivirus 2010 ... 199
25.2. Création d'un compte BitDefender ... 200

Intégration dans Windows et dans les logiciels tiers 204
26. Intégration dans le menu contextuel de Windows 205
26.1. Analyser avec BitDefender 205
27. Intégration dans les navigateurs Internet 207
28. Intégration dans les Programmes de Messagerie Instantanée ... 210
Comment faire pour 211
29. Comment analyser fichiers et dossiers 212
29.1. Utilisation du menu contextuel de Windows 212
29.2. Utilisation des tâches d'analyse 212
29.3. Utilisation de BitDefender Manual Scan 215
29.4. Utilisation de la barre d'activité d'analyse 216
30. Comment planifier l'analyse de l'ordinateur 217
Aide et résolution des problèmes 219
31. Résolution des problèmes 220
31.1. Problèmes d'installation 220
31.1.1. Erreurs de Validation de l'Installation 220
31.1.2. L'installation a échoué 221
31.2. Le Services BitDefender ne répondent pas 223
31.3. La désinstallation de BitDefender a échoué 223
32. Support Technique Editions Profil / BitDefender 225
BitDefender Rescue CD 228
33. Présentation 229
33.1. Configuration requise 229
33.2. Logiciels inclus 230
34. Comment utiliser le CD de secours BitDefender 233
34.1. Démarrer le CD de secours BitDefender 233
34.2. Arrêter le CD de secours BitDefender 234
34.3. Comment lancer une analyse antivirus ? 235
34.4. Comment configurer la connexion Internet? 236
34.5. Comment actualiser BitDefender? 237
34.5.1. Comment actualiser BitDefender via un proxy ? 238
34.6. Comment enregistrer mes données ? 239
34.7. Comment utiliser le mode console ? 241
Glossaire 242

Contrat de licence logiciel pour utilisateur final

Si vous n'acceptez pas les termes et conditions de cette licence, n'installez pas ce logiciel. En choisissant "J'accepte", "OK", "Continuer", "Oui", ou en installant ou en utilisant le logiciel de quelque manière que ce soit, vous confirmez que vous comprenez parfaitement et acceptez les termes de cette licence.

ENREGISTREMENT DU PRODUIT. En acceptant cet accord de licence, vous acceptez d'enregistrer votre logiciel, en utilisant "Mon compte" comme condition pour utiliser le logiciel (et recevoir les mises à jour) et bénéficier du support. Ce contrôle assure que le logiciel s'exécute uniquement sur des ordinateurs avec des clés de licence valides et que les utilisateurs identifiés aient bien accès aux services de support. L'enregistrement nécessite un code d'activation et un e-mail valides pour le renouvellement et autres notifications légales.

Les termes de cette licence incluent les Solutions et Service BitDefender pour votre usage personnel, y compris les documentations relatives aux produits, les mises à jour et mises à niveau des applications ou les services qui vous sont proposés dans le cadre de la licence, ainsi que toute reproduction de ces éléments.

Cet accord de licence est un accord légal entre vous (entité individuelle ou utilisateur final) et BITDEFENDER pour l'usage du produit de BITDEFENDER identifié au-dessus, qui comprend le logiciel et qui peut comprendre les éléments média, les matériels imprimés et la documentation "en ligne" ou électronique ("BitDefender"), le tout étant protégé par la loi française et par les lois et les traités internationaux. En installant, copiant, ou utilisant de toute autre manière le logiciel BitDefender, vous acceptez les termes de cet accord.

Si vous n'acceptez pas les termes de cette licence, n'installez pas ou n'utilisez pas BitDefender.

Accord de licence BitDefender. BitDefender est protégé par les lois sur les droits d'auteur et par les traités internationaux concernant le copyright, ainsi que par les autres lois et traités sur la propriété intellectuelle. BitDefender ne vous est pas vendu, la licence vous autorise seulement à l'utiliser.BitDefender est licencié et non pas vendu.

DROITS DE LICENCE. BITDEFENDER vous accorde à vous et vous seul cette licence d'utilisation BITDEFENDER non exclusive, limitée, non cessible, non transférable et non sous-licenciable.

LOGICIEL. Vous pouvez installer et utiliser BitDefender sur autant d'ordinateurs que nécessaire dans la limite imposée par le nombre d'utilisateurs prévus dans la licence. Vous pouvez faire une seule copie de sauvegarde.

LICENCE POUR ORDINATEUR. Cette licence s'applique au logiciel BitDefender qui peut être installé sur un ordinateur unique et ne fournit pas de services réseau. Chaque utilisateur principal peut installer ce logiciel sur un ordinateur unique et

faire une copie de sauvegarde sur un support différent. Le nombre d'utilisateurs principaux correspond au nombre d'utilisateurs prévu dans la licence.

DURÉE DE LA LICENCE. La licence accordée ci-dessus entrera en vigueur à la date d'achat et expirera à la fin de la période de validité.

EXPIRATION. Le produit cessera de fonctionner immédiatement à la date d'expiration de la licence.

MISES À JOUR. Si BitDefender constitue une mise à jour, vous devez être correctement licencié pour utiliser le produit identifié par BITDEFENDER comme étant éligible pour la mise à jour, afin d'utiliser BitDefender. Un produit BitDefender qui constitue une mise à jour remplace le produit qui formait la base de votre éligibilité pour la mise à jour. Vous pouvez utiliser le produit résultant seulement en accord avec les termes de cet Accord de licence. Si BitDefender est une mise à jour d'un composant d'un progiciel que vous avez acheté comme un seul produit, BitDefender peut être utilisé et transféré seulement comme une partie de ce progiciel et ne peut pas être séparé pour l'usage sur plus d'un ordinateur.Les termes et conditions de cette licence annule et remplace tout accord préalable ayant pu exister entre vous et BITDEFENDER concernant un produit complet ou un produit mis à jour.

COPYRIGHT. Tous les droits d'auteur de BitDefender (comprenant mais ne se limitant pas à toutes les images, photographies, logos, animations, vidéo, audio, musique, texte et " applets " compris dans BitDefender), les matériels imprimés qui l'accompagnent et les copies de BitDefender sont la propriété de BITDEFENDER. BitDefender est protégé par les lois concernant le copyright et par les traités internationaux. C'est pourquoi vous devez traiter BitDefender comme tout autre matériel protégé par le copyright à l'exception du fait que vous pouvez installer BitDefender sur un seul ordinateur, vu que vous gardez l'original seulement pour archive. Vous ne pouvez pas copier les matériels imprimés qui accompagnent BitDefender. Vous devez produire et inclure toutes les notices de copyright dans leur forme originale pour toutes les copies respectives du média ou de la forme dans laquelle BitDefender existe. Vous ne pouvez pas céder la licence, louer sous quelque forme que ce soit tout ou partie du logiciel BitDefender. Vous ne pouvez pas décompiler, désassembler, modifier, traduire ou tenter de découvrir le code source de ce logiciel ou créer des outils dérivés de BitDefender.

GARANTIE LIMITÉE. BITDEFENDER garantit que le support sur lequel le logiciel est distribué est exempt de vices de matériaux et de fabrication pendant une période de trente (30) jours à compter de la date de livraison du logiciel. Votre seul recours en cas de manquement à cette garantie sera le remplacement par BITDEFENDER du support défaillant durant la période de trente (30) jours à compter de la date de livraison du logiciel. BITDEFENDER ne garantit pas que le logiciel répondra à vos besoins ni qu'il fonctionnera sans interruption ou sans erreur. BITDEFENDER REFUSE TOUTE AUTRE GARANTIE POUR BITDEFENDER, QU'ELLE SOIT EXPRESSE OU IMPLICITE. LA GARANTIE CI-DESSUS EST EXCLUSIVE ET REMPLACE TOUTES AUTRES GARANTIES,

QU'ELLES SOIENT IMPLICITES OU EXPLICITES, Y COMPRIS LES GARANTIES IMPLICITES DE COMMERCIALISATION ET D'APPLICATION PARTICULIÈRE.

A l'exception des termes définis dans cet accord de licence, BITDEFENDER refuse toute autre forme de garantie, explicite ou implicite en rapport avec le produit, ses améliorations, sa maintenance, ou son support ainsi que tout autre matériel relatif (tangible ou intangible) ou service fournit par celui ci. BITDEFENDER refuse explicitement toutes garanties et conditions incluant, sans limitation, les garanties liées à la commercialisation, l'adaptation à un emploi particulier, la non interférence, la précision des données, la précision de contenus d'informations, l'intégration système, et la non violation des droits d'une tierce partie en filtrant, désactivant ou supprimant un logiciel, spyware, adware, des cookies, des emails, des documents, une publicité ou un autre produit du même type, d'une telle tierce partie, quel que soit leur mode d'utilisation.

EXCLUSION DE DOMMAGES. Quiconque utilise, teste ou évalue BitDefender assume tous les risques liés à la qualité et à la performance de BitDefender. En aucun cas BITDEFENDER ne pourra être tenu responsable de tout dommage tel qu'il soit, y compris, mais de manière non-limitative, de dommages directs ou indirects résultant de l'utilisation, de la performance ou de la livraison de BitDefender, et ce même si BITDEFENDER a été informé de la possibilité de tels dommages.

CERTAINS ÉTATS N'AUTORISENT PAS LA LIMITATION OU L'EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES INDIRECTS OU CONSÉCUTIFS, DE SORTE QUE LES LIMITATIONS CI-DESSUS PEUVENT NE PAS S'APPLIQUER À VOUS.

LA RESPONSABILITÉ DE BITDEFENDER NE SAURAIT EN AUCUN CAS DÉPASSER LA SOMME QUI A ÉTÉ DÉPENSÉE POUR L'ACHAT DE BITDEFENDER. Les exclusions et limitations énoncées ci-dessus s'appliquent indépendamment du fait que vous acceptez ou non d'utiliser, d'évaluer ou de tester BitDefender.

INFORMATION IMPORTANTE POUR LES UTILISATEURS. CE LOGICIEL N'EST PAS PREVU POUR DES MILIEUX DANGEREUX, DEMANDANT DES OPÉRATIONS OU UNE PERFORMANCE SANS ERREUR. CE LOGICIEL N'EST PAS RECOMMANDÉ DANS LES OPÉRATIONS DE NAVIGATION AÉRIENNE, INSTALLATIONS NUCLÉAIRES OU DES SYSTÈMES DE COMMUNICATION, SYSTÈMES D'ARMEMENT, SYSTÈMES ASSURANT DIRECTEMENT OU INDIRECTEMENT LE SUPPORT VITAL, CONTROLE DU TRAFFIC AÉRIEN, OU TOUTE AUTRE APPLICATION OU INSTALLATION OU LA DÉFAILLANCE POURRAIT AVOIR COMME EFFET LA MORT DES PERSONNES, DES BLESSURES PHYSIQUES SÉVÈRES OU DES DOMMAGES DE LA PROPRIÉTÉ.

ACCORD CONCERNANT LES INFORMATIONS ÉLECTRONIQUES. BitDefender peut avoir à vous envoyer des informations juridiques ou autres, au sujet du logiciel et des services associés à BitDefender ainsi que concernant l'utilisation qui peut être faite des informations que vous nous avez communiquées. BitDefender enverra ces informations sous forme de message via le produit lui même ou par e-mail (en utilisant les coordonnées enregistrés lors de la création de votre compte) ou publiera des informations sur son site Internet. En acceptant cet Accord, vous acceptez de

recevoir des informations sous forme électronique et reconnaissez avoir connaissance que ces informations sont disponibles sur les sites Internet de BitDefender.

TECHNOLOGIE DE COLLECTE DE DONNÉES- . BitDefender vous informe qu'il peut utiliser dans certains programmes ou produits une technologie de collecte de données afin d'obtenir des informations techniques (y compris des fichiers suspects) pour améliorer ses produits, offrir des services associés, les adapter, ainsi que pour empêcher toute utilisation illégale ou sans licence du produit, ou des dommages résultants de malwares. Vous acceptez que BitDefender puisse utiliser ces informations pour les services proposés liés au produit et pour empêcher et stopper l'exécution de malwares sur votre ordinateur.

Vous reconnaissez et acceptez que BitDefender puisse procéder à des modifications du programme ou du produit ou à des ajouts qui seront téléchargés automatiquement sur votre ordinateur.

En acceptant cet accord de licence, vous acceptez de télécharger les fichiers exécutables afin d'être analysé par les serveurs de BitDefender. De même, pour contracter et utiliser le programme, vous devez fournir à BitDefender certaines données personnelles. BitDefender vous informe qu'il traitera vos données personnelles dans le respect de la législation actuelle et comme stipulé dans son Accord de Confidentialité.

RECUEIL DE DONNÉES. L'accès de l'utilisateur au site Internet, l'acquisition de produits et de services ainsi que l'utilisation d'outils ou de contenu via le site Internet implique le traitement de données personnelles. Le respect de la législation régissant le traitement des données personnelles, les services de la société d'information et le commerce électronique est de la plus haute importance pour BitDefender. Parfois, pour accéder aux produits, aux contenus ou aux outils des services, vous devrez indiquer certaines données personnelles. BitDefender garantit que ces données seront traitées en toute confidentialité dans le respect de la législation régissant la protection des données personnelles, les services de la société de l'information et le commerce électronique.

BitDefender respecte la législation de protection des données et a mis en place les mesures techniques et administratives nécessaires pour garantir la sécurité des données personnelles recueillies.

Vous garantissez la véracité et l'exactitude des données que vous soumettez et vous engagez à informer BitDefender de tout changement de ces données. Vous avez le droit de vous opposer au traitement des données non essentielles à l'exécution de cet accord et à leur utilisation dans un but autre que la maintenance de cette relation contractuelle.

Si les données que vous indiquez appartiennent à un tiers, BitDefender ne saurait être tenu responsable du respect des principes d'informations et de consentement, et vous devez donc garantir que vous avez informé au préalable le propriétaire des données et obtenu son accord pour communiquer ces données.

BitDefender, ses affiliés et partenaires enverront uniquement des informations de marketing par e-mail ou par d'autres moyens électroniques aux utilisateurs ayant donné leur consentement explicite pour recevoir des informations concernant les produits, les services ou les newsletters de BitDefender.

Vous disposez d'un droit d'accès, de rectification et de suppression des données vous concernant et pouvez vous opposer au traitement de ces données en le notifiant à BitDefender par e-mail à l'adresse suivante : juridic@bitdefender.com.

CONDITIONS GÉNÉRALES. Cet accord est régi par les lois de la Roumanie et par les règlements et les traités internationaux concernant le copyright. La seule juridiction compétente en cas de désaccord concernant cet accord de licence sera la Cour de justice de Roumanie.

Dans l'éventualité d'une invalidité de tout règlement de cet Accord, cette invalidité n'affectera pas la validité du reste de cet Accord.

BitDefender et le logo de BitDefender sont des marques déposées de BITDEFENDER. Toutes les autres marques et produits associés appartiennent à leurs propriétaires respectifs.

La licence prendra fin immédiatement sans qu'il soit besoin de vous avertir si vous ne respectez pas une ou plusieurs des conditions édictées dans cet accord. Il ne vous sera pas possible de demander un remboursement de la part de BITDEFENDER ou d'un de ses représentants en cas de cloture de cette licence. Les termes et conditions de respect de confidentialité et leurs restrictions doivent rester de mise même après la fin du contrat.

BITDEFENDER s'autorise à revoir quand il le souhaite les termes de cette licence, ceux ci s'appliqueront automatiquement aux produits distribués qui incluent les termes modifiés. Dans l'éventualité d'une invalidité d'une partie de cet accord, cette invalidité n'affectera pas la validité du reste de cet Accord.

En cas de controverses ou d'incohérence dans la traduction des termes de cette licence dans une autre langue, seule la version anglaise édité par BITDEFENDER sera déclarée valide.

Pour contacter BITDEFENDER : West Gate Park, Building H2, 24, Preciziei Boulevard, Sector 6, Bucarest, Roumanie, Téléphone : +40-21-3001255 ou +40-21-3001254, e-mail: office@bitdefender.com. Pour contacter EDITIONS PROFIL : 49 Rue de la Vanne 92120 Montrouge - FRANCE, Téléphone : 01 47 35 72 73, E-mail : bitdefender@editions-profil.eu.

Préface

Ce Manuel d'utilisation est destiné à tous les utilisateurs qui ont choisi **BitDefender Antivirus 2010** comme solution de sécurité pour leur ordinateur personnel. Les informations présentées dans ce livret sont destinées aussi bien aux utilisateurs expérimentés en informatique qu'à toute personne sachant utiliser Windows.

Vous trouverez dans ce manuel une description de BitDefender Antivirus 2010, le guide de son installation, et toutes les indications nécessaires à sa configuration. Vous découvrirez comment utiliser BitDefender Antivirus 2010, l'actualiser, le tester et le personnaliser. Vous apprendrez comment exploiter au mieux toutes les ressources de BitDefender.

Nous vous souhaitons un apprentissage agréable et utile.

1. Conventions utilisées dans ce manuel

1.1. Normes Typographiques

Plusieurs styles de texte sont utilisés dans ce livret pour une lisibilité améliorée. Leur aspect et signification sont présentés dans le tableau ci dessous.

Apparence	Description
`sample syntax`	Les exemples de syntaxe sont imprimés avec des caractères `séparés d'un espace`.
http://www.bitdefender.fr	Les liens URL pointent vers un emplacement externe comme un serveur http ou ftp.
documentation@bitdefender.com	Les adresses Email sont insérées dans le texte pour plus d'informations sur les contacts.
« Préface » (p. xiv)	Ceci représente un lien interne vers un emplacement à l'intérieur de ce document.
`filename`	Les fichiers et répertoires sont imprimés en utilisant des caractères `séparés d'un espace`.
option	Toutes les informations sur le produit sont imprimées en utilisant des caractères **Gras**.
`sample code listing`	La liste de code est imprimée avec des caractères `séparés d'un espace`.

1.2. Avertissements

Les avertissements sont des notes textes graphiquement marquées, offrant à votre attention des informations additionnelles relatives au paragraphe actuel.

Note
La note est une courte observation. Bien que vous puissiez l'omettre, les notes apportent des informations non négligeables, comme des fonctions spécifiques ou un lien à un thème proche.

Important
Cette icône requiert votre attention et nous vous recommandons de ne pas l'ignorer. Elle fournit habituellement des informations non critiques mais significatives.

Avertissement
Marque une information critique que vous devrez lire attentivement. Rien de négatif ne se passera si vous suivez les indications. Vous devriez le lire et le comprendre car cette marqué décrit une opération risquée.

2. Structure du manuel

Le manuel est composé de plusieurs parties reprenant les thèmes principaux. S'y ajoute un glossaire pour l'éclaircissement de certains termes techniques.

Installation et désinstallation. Instructions pour installer BitDefender sur un ordinateur personnel. Elles débutent par les conditions préalables à une installation réussie, et vous guident tout au long du processus d'installation. Enfin, la procédure de désinstallation est décrite au cas où vous auriez besoin de désinstaller BitDefender.

Pour démarrer. Contient toutes les informations dont vous avez besoin pour commencer à utiliser BitDefender. Vous découvrirez l'interface BitDefender et comment corriger des problèmes, configurer des paramètres de base et enregistrer votre produit.

Mode Intermédiaire. Présente l'interface en Mode Intermédiaire de BitDefender.

Mode Expert. Présentation détaillée de l'interface Expert de BitDefender. Vous apprendrez à configurer et à utiliser tous les modules BitDefender afin de protéger efficacement votre ordinateur contre toutes les menaces de codes malveillants (virus, spyware, rootkits, etc.).

Intégration dans Windows et dans les logiciels tiers. Vous montre comment utiliser les options de BitDefender dans le menu contextuel de Windows et les barres d'outils BitDefender intégrées dans les programmes tiers pris en charge.

Comment faire pour. Donne la marche à suivre pour exécuter rapidement les tâches les plus courantes dans BitDefender.

Aide et résolution des problèmes. Où regarder et à qui demander de l'aide si quelque chose d'inattendu apparaît.

BitDefender Rescue CD. Description du CD de secours BitDefender. Elle aide à comprendre et à utiliser les fonctionnalités proposées par ce CD bootable.

Glossaire. Le glossaire tente de vulgariser des termes techniques et peu communs que vous trouverez dans ce document.

3. Commentaires

Nous vous invitons à nous aider à améliorer ce livret. Nous avons testé et vérifié toutesles informations mais vous pouvez trouver que certaines fonctions ont changé.N'hésitez pas à nous écrire pour nous dire si vous avez trouvé des erreurs dans celivret ou concernant toute amélioration que nous pourrions y apporter pour vous fournirla meilleure documentation possible.

Faites le nous savoir en nous écrivant à cette adresse documentation@bitdefender.com.

Important

Merci de bien vouloir rédiger en anglais vos e-mails concernant cette documentation afin que nous puissions les traiter efficacement.

Installation et désinstallation

1. Configuration requise

Vous pouvez installer BitDefender Antivirus 2010 uniquement sur les ordinateurs fonctionnant avec les systèmes d'exploitation suivants :

- Windows XP (32/64 bits)avec Service Pack 2 ou supérieur
- Windows Vista (32/64 Bit) ou Windows Vista avec Service Pack 1 ou supérieur
- Windows 7 (32/64 bits)

Avant d'installer le produit, vérifiez que le système remplit les conditions minimales suivantes :

Note

Pour vérifier quel système d'exploitation fonctionne actuellement sur votre ordinateur ainsi que des informations sur votre matériel, faites un clic-droit sur **Poste de travail** et sélectionnez **Propriétés** dans le menu.

1.1. Configuration système minimale

- 450 Mo d'espace disque disponible
- Processeur 800MHz
- Mémoire RAM :
  - 512 Mo pour Windows XP
  - 1 Go pour Windows Vista et Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (également disponible dans le kit d'installation)

1.2. Configuration système recommandée

- 600 Mo d'espace disque disponible
- Intel CORE Duo (1,66 GHz) ou processeur équivalent
- Mémoire RAM :
  - 1 Go pour Windows XP et Windows 7
  - 1,5 Go pour Windows Vista
- Internet Explorer 7 (ou version supérieure)
- .NET Framework 1.1 (également disponible dans le kit d'installation)

1.3. Logiciels pris en charge

La protection antiphishing est seulement disponible pour :

- Internet Explorer 6.0 (ou version supérieure)
- Mozilla Firefox 2.5
- Yahoo Messenger 8.5
- Windows Live Messenger 8

Le cryptage des messageries instantanées est disponible seulement pour :

- Yahoo Messenger 8.5
- Windows Live Messenger 8

2. Préparation de l'Installation

Avant d'installer BitDefender Antivirus 2010, procédez comme suit pour faciliter l'installation :

- Vérifiez que l'ordinateur où vous prévoyez d'installer BitDefender dispose de la configuration minimale requise. Si l'ordinateur ne dispose pas de la configuration minimale requise, BitDefender ne pourra pas être installé, ou, une fois installé, il ne fonctionnera pas correctement, ralentira le système et le rendra instable. Pour des informations détaillées sur la configuration nécessaire, veuillez consulter « *Configuration requise* » (p. 2).
- Connectez-vous à l'ordinateur en utilisant un compte Administrateur.
- Désinstallez tous les logiciels de sécurité de l'ordinateur. L'exécution de deux programmes de sécurité à la fois peut affecter leur fonctionnement et provoquer d'importants problèmes avec le système. Windows Defender sera désactivé par défaut avant le début de l'installation.

2.1. Installation de BitDefender sur un NetBook/Mini-PC

BitDefender Antivirus 2010 peut être installé sur 1 ou 3 ordinateurs situés à une même adresse postale.

Si vous utilisez un Mini-PC vous disposez de deux solutions au choix pour installer votre produit BitDefender :

- Insérez le DVD-Rom de BitDefender 2010 dans le lecteur de DVD d'un PC en disposant. Après le lancement de la fenêtre d'installation, sélectionnez le produit BitDefender correspondant à votre achat, choisissez **Copier vers un disque USB** pour copier les fichiers d'installation des BitDefender vers un périphérique USB que vous pourrez ensuite utiliser sur votre Mini-PC. Copiez les fichiers d'installation sur votre Mini-PC, installez votre produit BitDefender et activez-le avec la clé de licence fournie avec votre achat.
- Téléchargez le produit BitDefender 2010 correspondant à votre achat directement depuis le navigateur Internet de votre Mini-PC sur le site : www.bitdefender.fr dans la rubrique **Téléchargement**. Installez ensuite votre produit BitDefender et activez-le avec la clé de licence fournie avec votre achat.

3. Installation de BitDefender

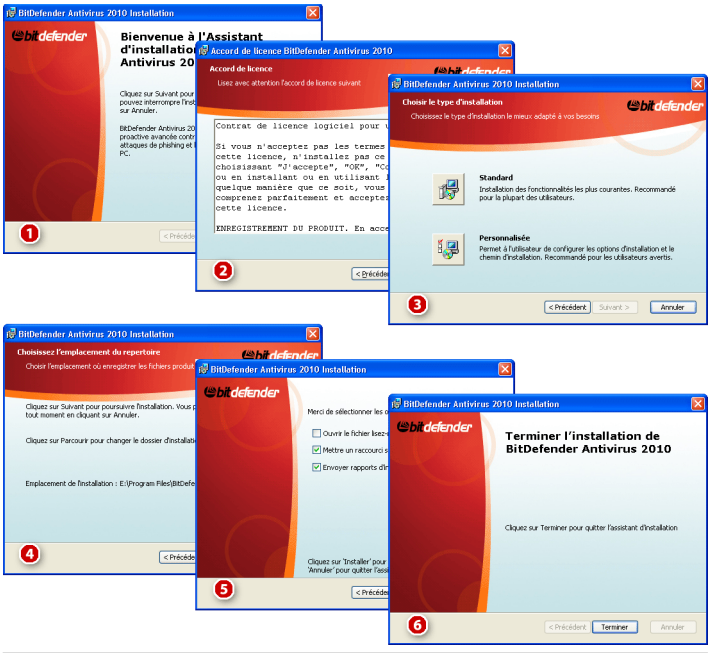
Vous pouvez installer BitDefender à partir de son CD d'installation ou en utilisant un fichier d'installation téléchargé sur votre ordinateur à partir du site Internet de BitDefender ou d'autres sites Internet autorisés (par exemple, le site d'un partenaire de BitDefender ou une boutique en ligne). Vous pouvez télécharger le fichier d'installation sur le site Internet de BitDefender à l'adresse suivante : http://www.bitdefender.fr/site/Downloads/.

- Pour installer BitDefender à partir du CD, insérez le CD dans le lecteur. Un écran d'accueil s'affiche peu après. Suivez les instructions pour lancer l'installation.

  Si l'écran d'accueil n'apparaît pas, suivez le chemin : `Products\Antivirus\install\fr\` à partir du répertoire racine du CD et double-cliquez sur `runsetup.exe`.

- Pour installer BitDefender en utilisant le fichier d'installation téléchargé sur votre ordinateur, localisez le fichier et double-cliquez dessus.

Le programme d'installation vérifiera d'abord votre système pour valider l'installation. Si l'installation est validée, l'assistant de configuration apparaîtra. L'image suivante présente les étapes de l'assistant de configuration.



Étapes d'installation

Voici les étapes à suivre pour installer BitDefender Antivirus 2010 :

1. Cliquez sur **Suivant**. Vous pouvez annuler l'installation à tout moment en cliquant sur **Annuler**.

   BitDefender Antivirus 2010 vous prévient si d'autres produits antivirus sont installés sur votre ordinateur. Cliquez sur **Supprimer** pour désinstaller le produit correspondant. Si vous souhaitez poursuivre sans supprimer le produit détecté, cliquez sur **Suivant**.

   Avertissement
   Il est fortement recommandé de désinstaller les autres antivirus avant d'installer BitDefender. Faire fonctionner plusieurs antivirus sur le même ordinateur le rend généralement inutilisable.

2. Veuillez lire les accords de licence et cliquez sur **J'accepte**.

   Important
   Si vous être en désaccord avec les termes du contrat, cliquez sur **Annuler**. Le processus sera interrompu et vous quitterez l'installation.

3. Sélectionnez le type d'installation à réaliser.
   - **Standard** - pour installer le programme immédiatement, en utilisant les options d'installation par défaut. Si vous choisissez cette option, passez directement à l'étape 6.
   - **Personnalisé** - pour configurer les options d'installation avant d'installer le programme. Cette option vous permet de modifier le répertoire d'installation.
4. Par défaut, BitDefender Antivirus 2010 sera installé dans `C:\Program Files\BitDefender\BitDefender 2010`. Si vous voulez choisir un autre répertoire, cliquez sur **Parcourir** et choisissez le répertoire d'installation.

   Cliquez sur **Suivant**.
5. Sélectionnez les options du processus d'installation. Les options recommandées sont sélectionnées par défaut :
   - **Ouvrir le fichier lisezmoi** - pour ouvrir le fichier lisezmoi à la fin de l'installation.
   - **Créer un raccourci sur le bureau** - pour placer un raccourci BitDefender Antivirus 2010 sur le bureau à la fin de l'installation.
   - **Désactiver la mise en cache DNS** - pour désactiver la mise en cache DNS (système de noms de domaine) Le service Client DNS peut être utilisé par des applications malveillantes pour envoyer des informations à travers le réseau sans votre consentement.
   - **Envoyer des Rapports d'infection** - permet d'envoyer des rapports d'infection aux Laboratoires BitDefender pour analyse. Veuillez noter que ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et ne seront pas utilisés à des fins commerciales.
   - **Désactiver Windows Defender** - pour désactiver Windows Defender ; cette option n'est disponible que sous Windows Vista.

   Cliquez sur **Installer** pour lancer l'installation du programme. Si il n'est pas déjà installé, BitDefender commencera par installer .NET Framework 1.1.
6. Patientez jusqu'à ce que l'installation soit complète puis cliquez sur **Terminer**. Il vous sera peut être demandé de redémarrer votre système pour terminer le processus d'installation. Il est recommandé de le faire dès que possible

Important

Après avoir effectué l'installation et redémarré l'ordinateur, un assistant d'enregistrement et un assistant de configuration apparaîtront. Utilisez ces assistants pour enregistrer et configurer BitDefender Antivirus 2010 ainsi que pour créer un compte BitDefender.

Si vous avez accepté les paramètres par défaut pour le répertoire d'installation, vous pouvez voir dans `Program Files` un nouveau répertoire, nommé `BitDefender`, qui contient le sous-dossier `BitDefender 2010`.

3.1. Assistant d'enregistrement

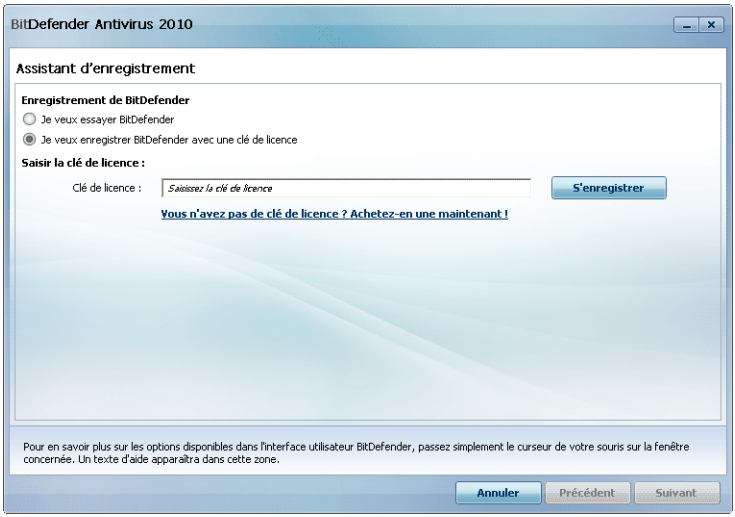
La première fois que vous démarrerez l'ordinateur après l'installation, un assistant d'enregistrement apparaîtra. Cet assistant vous aide à enregistrer votre produit et à configurer un compte BitDefender.

Vous devez créer un compte BitDefender afin de recevoir les mises à jour BitDefender. Le compte BitDefender vous donne accès au support technique gratuit, à des offres spéciales et à des promotions. Si vous perdez votre clé d'activation BitDefender, vous pouvez la retrouver en vous connectant sur votre compte à l'adresse http://myaccount.bitdefender.com.

Note

Si vous ne voulez pas utiliser cet assistant, cliquez sur **Annuler**. Vous pouvez ouvrir l'assistant d'enregistrement n'importe quand en cliquant sur le lien **Enregistrer**, situé en bas de l'interface du produit.

3.1.1. Étape 1 - Enregistrer BitDefender Antivirus 2010


BitDefender Antivirus 2010
Assistant d'enregistrement
Enregistrement de BitDefender
Je veux essayer BitDefender
Je veux enregistrer BitDefender avec une clé de licence
Saisir la clé de licence :
Clé de licence :
Saisissez la clé de licence
S'enregistrer
Vous n'avez pas de clé de licence ? Achetez-en une maintenant !
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Suivant

Enregistrement

BitDefender Antivirus 2010 a une période d'essai de 30 jours. Pour continuer à essayer le produit, sélectionnez **Je veux essayer BitDefender** et cliquez sur **Suivant**.

Pour enregistrer BitDefender Antivirus 2010 :

1. Sélectionnez **Je veux enregistrer BitDefender avec une nouvelle clé**.
2. Entrez la clé d'activation dans le champ de saisie.

Note

Vous trouverez votre clé d'activation :

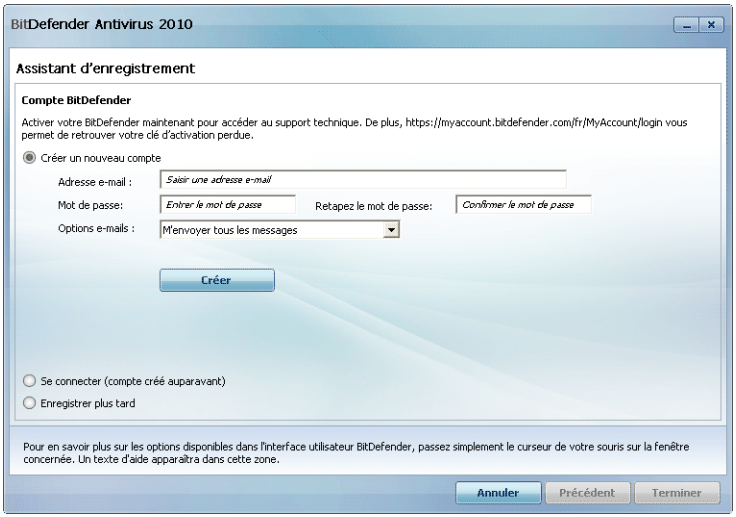
- sur l'étiquette du CD.
- sur la carte d'enregistrement du produit.
- sur l'e-mail d'achat en ligne.

Si vous n'avez pas de clé d'activation BitDefender, cliquez sur le lien indiqué pour être dirigé vers la boutique en ligne BitDefender et en acheter une.

3. Cliquez sur **S'enregistrer**.
4. Cliquez sur **Suivant**.

Si une clé de licence BitDefender valide est détectée sur votre système, vous pouvez continuer à l'utiliser en cliquant sur **Suivant**.

3.1.2. Etape 2 - Création d'un compte BitDefender


BitDefender Antivirus 2010
Assistant d'enregistrement
Compte BitDefender
Activer votre BitDefender maintenant pour accéder au support technique. De plus, https://myaccount.bitdefender.com/fr/MyAccount/login vous permet de retrouver votre clé d'activation perdue.
Créer un nouveau compte
Adresse e-mail :
Saisir une adresse e-mail
Mot de passe:
Entrer le mot de passe
Retapez le mot de passe:
Confirmer le mot de passe
Options e-mails :
M'envoyer tous les messages
Créer
Se connecter (compte créé auparavant)
Enregistrer plus tard
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Terminer

Création de compte

Si vous ne souhaitez pas créer immédiatement un compte BitDefender, sélectionnez **Enregistrer plus tard** et cliquez sur **Terminer**. Autrement, procédez selon votre situation actuelle :

- « Je n'ai pas de compte BitDefender » (p. 10)
- « J'ai déjà un compte BitDefender » (p. 11)

Important

Vous devez créer un compte dans les 15 jours après l'installation de BitDefender (si vous l'enregistrez avec une clé de licence, l'expiration est repoussée à 30 jours). Dans le cas contraire, BitDefender ne se mettra plus à jour.

Je n'ai pas de compte BitDefender

Pour créer un compte BitDefender, suivez ces étapes :

1. Sélectionnez **Créer un nouveau compte**.
2. Tapez les informations requises dans les champs correspondants. Les informations communiquées ici resteront confidentielles.
   - **E-mail** - entrez votre adresse e-mail.

- **Mot de passe** - entrez un mot de passe pour votre compte BitDefender. Le mot de passe doit contenir entre 6 et 16 caractères.
- **Retaper le mot de passe** - re-entrez le mot de passe choisi auparavant.

Note
Une fois le compte activé, vous pouvez utiliser l'adresse e-mail et le mot de passe indiqués pour vous connecter à votre compte sur http://myaccount.bitdefender.com.

3. Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte. Sélectionnez l'une des options disponibles dans le menu :
   - **M'envoyer tous les messages**
   - **M'envoyer seulement les messages concernant le produit**
   - **Je ne veux recevoir aucun message**
4. Cliquez sur **Créer**.
5. Cliquez sur **Terminer** pour quitter l'assistant.
6. **Activez votre compte.** Vous devez activez votre compte avant de pouvoir l'utiliser. Consultez votre messagerie et suivez les instructions données dans le message que vous a adressé le service d'enregistrement de BitDefender.

J'ai déjà un compte BitDefender

BitDefender détectera automatiquement si vous avez déjà un compte BitDefender actif sur cet ordinateur. Dans ce cas, indiquez le mot de passe de votre compte et cliquez sur **Se connecter**. Cliquez sur **Terminer** pour quitter l'assistant.

Si vous avez déjà un compte actif, mais que BitDefender ne le détecte pas, suivez ces étapes pour enregistrer le produit avec ce compte :

1. Sélectionnez **Se connecter (compte créé auparavant)**.
2. Tapez l'adresse e-mail et le mot de passe de votre compte dans les champs correspondants.

Note
Si vous ne souhaitez pas faire de modifications, cliquez sur **Terminer** pour fermer l'assistant.

3. Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte. Sélectionnez l'une des options disponibles dans le menu :
   - **M'envoyer tous les messages**
   - **M'envoyer seulement les messages concernant le produit**
   - **Je ne veux recevoir aucun message**

4. Cliquez sur **Se connecter**.
5. Cliquez sur **Terminer** pour quitter l'assistant.

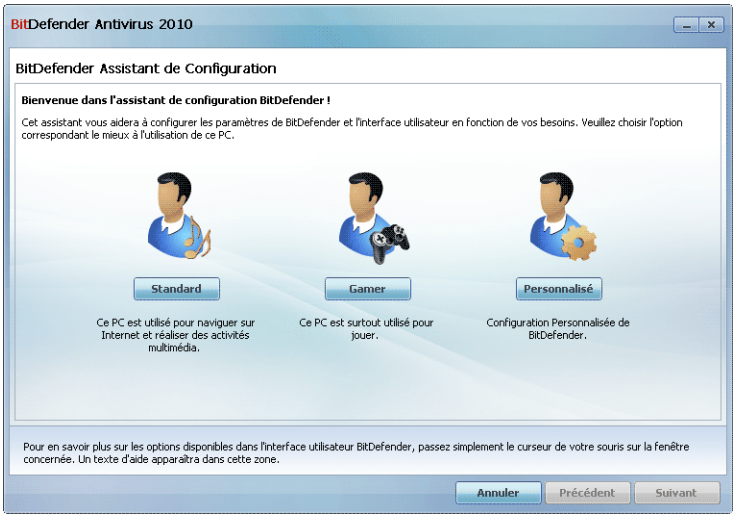
3.2. Assistant de configuration

Une fois l'enregistrement terminé, un assistant de configuration s'affiche. Cet assistant vous aide à configurer les principaux paramètres de BitDefender et l'interface utilisateur afin qu'ils répondent mieux à vos attentes. À la fin de l'assistant, vous pouvez mettre à jour les fichiers du produit et les signatures de codes malveillants et analyser les applications et les fichiers du système pour vous assurer qu'ils ne sont pas infectés.

L'assistant consiste en quelques étapes simples. Le nombre d'étapes dépend des choix que vous faites. Toutes les étapes sont présentées ici, mais vous serez averti(e) si vos choix affectent leur nombre.

Utiliser cet assistant n'est pas obligatoire. Cependant, nous vous recommandons de le faire pour gagner du temps et vous assurer que votre système est sain avant l'installation de BitDefender Antivirus 2010. Si vous ne voulez pas utiliser cet assistant, cliquez sur **Annuler**. BitDefender vous avertira des éléments que vous avez besoin de configurer quand vous ouvrirez l'interface utilisateur.

3.2.1. Étape 1 - Sélectionner le Profil d'Utilisation


BitDefender Antivirus 2010
BitDefender Assistant de Configuration
Bienvenue dans l'assistant de configuration BitDefender !
Cet assistant vous aidera à configurer les paramètres de BitDefender et l'interface utilisateur en fonction de vos besoins. Veuillez choisir l'option correspondant le mieux à l'utilisation de ce PC.
Standard
Ce PC est utilisé pour naviguer sur Internet et réaliser des activités multimédia.
Gamer
Ce PC est surtout utilisé pour jouer.
Personnalisé
Configuration Personnalisée de BitDefender.
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Suivant

Profils d'Utilisation

Cliquez sur le bouton qui décrit le mieux les activités réalisées avec cet ordinateur (le profil d'utilisation).

Option	Description
Standard	Cliquez ici si vous utilisez ce PC principalement pour naviguer sur Internet et réaliser des activités multimédia.
Gamer	Cliquez ici si ce PC est surtout utilisé pour jouer.
Personnalisé	Cliquez ici si vous voulez configurer tous les principaux paramètres de BitDefender.

Vous pourrez ensuite réinitialiser le profil d'utilisation à partir de l'interface du produit.

3.2.2. Étape 2 - Description de l'ordinateur

BitDefender Antivirus 2010
BitDefender Assistant de Configuration
Choisissez l'option à appliquer à ce PC
Cette étape vous permet de configurer la Gestion du Réseau Personnel BitDefender et le Mode Portable. Veuillez cocher les cases correspondant à la description de ce PC.
Cet ordinateur fait partie d'un réseau personnel
Sélectionnez cette option si vous voulez avoir accès facilement à partir de l'interface utilisateur au module de Gestion du Réseau Personnel. Ce module vous permet de gérer d'autres produits BitDefender de votre réseau personnel, à distance.
Cet ordinateur est un ordinateur portable
Sélectionnez cette option si vous voulez que le Mode Ordinateur Portable soit activé par défaut. Il permet à la batterie de votre ordinateur portable de durer plus longtemps, en évitant l'exécution de tâches requérant des ressources supplémentaires.
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Suivant

Description de l'ordinateur

Sélectionnez les options qui s'appliquent à votre ordinateur :

- **Cet ordinateur fait partie d'un réseau personnel.** Sélectionnez cette option si vous souhaitez gérer le produit BitDefender que vous avez installé sur cet ordinateur à distance (à partir d'un autre ordinateur) Une étape supplémentaire de l'assistant vous permettra de configurer le module de Gestion du Réseau Personnel.
- **Cet ordinateur est un ordinateur portable.** Sélectionnez cette option si vous souhaitez que le Mode Portable soit activé par défaut. En Mode Portable, les tâches d'analyse planifiées ne sont pas effectuées car elles nécessitent plus de ressources système et donc, réduisent l'autonomie de la batterie.

Cliquez sur **Suivant** pour continuer.

3.2.3. Étape 3 - Sélectionner l'Interface Utilisateur

BitDefender Antivirus 2010
BitDefender Assistant de Configuration
Choisissez le type d'utilisateur qui correspond le mieux à vos besoins
Cette étape vous permet de définir comment vous souhaitez que BitDefender fonctionne et le niveau de contrôle que vous souhaitez avoir sur les actions du programme. Sélectionnez l'option qui vous correspond le mieux.
Débutant
Très simple d'utilisation. Interface utilisateur minimale. BitDefender prend toutes les décisions pour vous.
Intermédiaire
Contrôle des paramètres de base. Interface Utilisateur classique. Vous prenez les décisions principales.
Expert
Contrôle de tous les paramètres. Interface Utilisateur Expert. Vous prenez toutes les décisions concernant le programme.
Si vous sélectionnez cette option, l'interface utilisateur de BitDefender sera en mode Expert. Vous pourrez passer en mode Intermédiaire ou Débutant à tout moment en allant dans Paramètres > Modifier le mode de l'interface utilisateur.
Annuler
Précédent
Suivant

Modes d'affichage de l'interface utilisateur

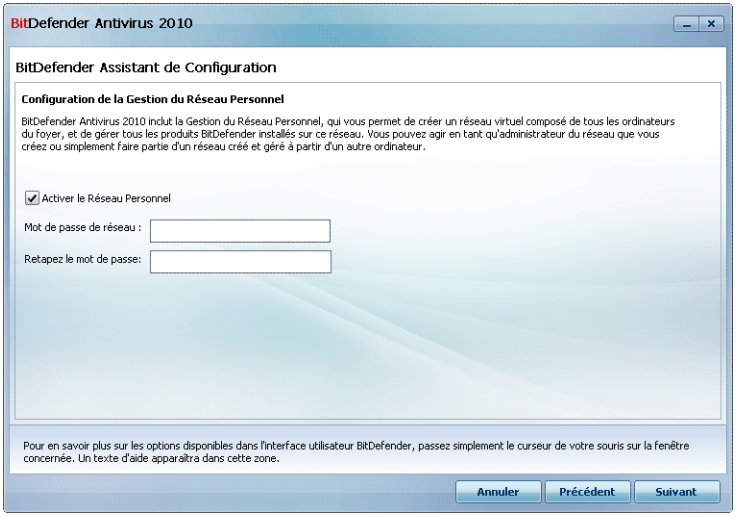
Cliquez sur le bouton qui décrit le mieux vos compétences en informatique pour sélectionner le mode de l'interface utilisateur approprié. Vous pouvez choisir d'afficher l'interface utilisateur avec l'un des trois modes, en fonction de vos compétences en informatique et de votre connaissance de BitDefender.

Mode	Description
Mode Débutant	Convient aux débutants en informatique et aux personnes qui souhaitent que BitDefender protège leur ordinateur et leurs données sans être interrompues. Ce mode est facile à utiliser et ne requiert de votre part que très peu d'interventions. Vous devez simplement corriger les problèmes rencontrés comme indiqué par BitDefender. Un assistant intuitif vous guidera pas à pas dans la résolution de ces problèmes. Vous pouvez également réaliser des tâches courantes comme la mise à jour des signatures de virus BitDefender et des fichiers du programme ou l'analyse de l'ordinateur.
Mode Intermédiaire	Conçu pour des utilisateurs ayant des compétences moyennes en informatique, ce mode étend les possibilités du Mode Débutant.

Mode	Description
	Vous pouvez corriger les problèmes séparément et choisir les éléments à surveiller. De plus, vous pouvez gérer à distance les produits BitDefender installés sur les ordinateurs de votre foyer.
Mode Expert	Ce mode, qui convient à des utilisateurs ayant plus de connaissances techniques, vous permet de configurer en détail chaque fonctionnalité de BitDefender. Vous pouvez également utiliser toutes les tâches fournies pour protéger votre ordinateur et vos données.

3.2.4. Étape 4 - Configurer le Réseau BitDefender

Note
Cette étape apparaît uniquement si vous avez indiqué à l'Étape 2 que l'ordinateur est connecté à un réseau domestique.


BitDefender Antivirus 2010
BitDefender Assistant de Configuration
Configuration de la Gestion du Réseau Personnel
BitDefender Antivirus 2010 inclut la Gestion du Réseau Personnel, qui vous permet de créer un réseau virtuel composé de tous les ordinateurs du foyer, et de gérer tous les produits BitDefender installés sur ce réseau. Vous pouvez agir en tant qu'administrateur du réseau que vous créez ou simplement faire partie d'un réseau créé et géré à partir d'un autre ordinateur.
Activer le Réseau Personnel
Mot de passe de réseau :
Retapez le mot de passe:
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Suivant

Configuration du réseau BitDefender

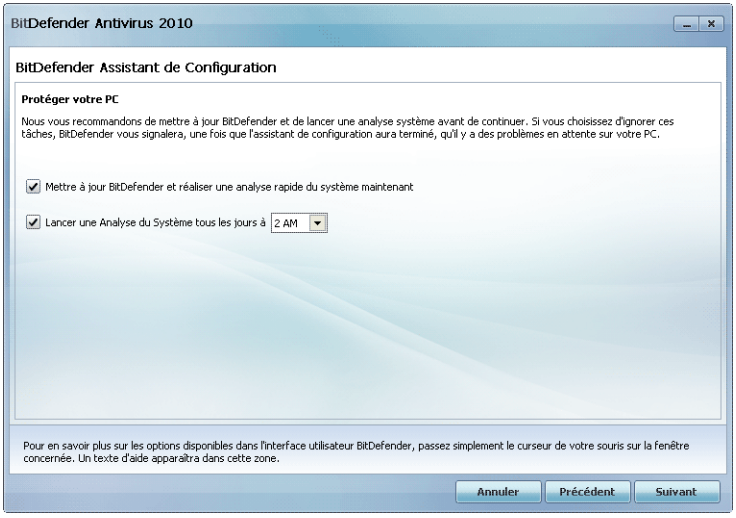
BitDefender vous permet de créer un réseau virtuel rassemblant tous les ordinateurs de votre foyer, et de gérer ensuite les produits BitDefender installés sur ce réseau.

Si vous voulez que cet ordinateur fasse partie du réseau personnel BitDefender, suivez ces étapes :

1. Sélectionnez **Activer le Réseau Personnel**.
2. Entrez le même mot de passe d'administration dans chacun des champs de saisie. Ce mot de passe permet à l'administrateur de gérer le produit BitDefender à partir d'un autre ordinateur.

Cliquez sur **Suivant** pour continuer.

3.2.5. Étape 5 - Sélectionner les tâches à exécuter


BitDefender Antivirus 2010
BitDefender Assistant de Configuration
Protéger votre PC
Nous vous recommandons de mettre à jour BitDefender et de lancer une analyse système avant de continuer. Si vous choisissez d'ignorer ces tâches, BitDefender vous signalera, une fois que l'assistant de configuration aura terminé, qu'il y a des problèmes en attente sur votre PC.
Mettre à jour BitDefender et réaliser une analyse rapide du système maintenant
Lancer une Analyse du Système tous les jours à 2 AM
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Suivant

Sélection des tâches

Paramètrez BitDefender pour lancer les tâches de sécurité importantes pour votre ordinateur. Voici les options proposées :

- **Mettre à jour BitDefender et réaliser une analyse rapide du système maintenant** - pendant la prochaine étape, les signatures de virus et les fichiers du produit BitDefender seront mis à jour afin de protéger votre ordinateur contre les nouvelles menaces. Dès la mise à jour terminée, BitDefender analysera les fichiers des dossiers `Windows` et `Program Files` pour s'assurer qu'ils ne sont pas infectés. Ces dossiers contiennent des fichiers du système d'exploitation et des applications installées et sont généralement les premiers à être infectés.
- **Lancer une Analyse du Système tous les jours à 2 heures** - configure BitDefender pour qu'il lance une analyse standard de votre ordinateur tous les jours à 2 h. Pour modifier l'heure de l'analyse, cliquez sur le menu et sélectionnez l'heure de début désirée. Si l'ordinateur est éteint au moment prévu, l'analyse s'exécutera la prochaine fois que vous l'allumerez.

Note

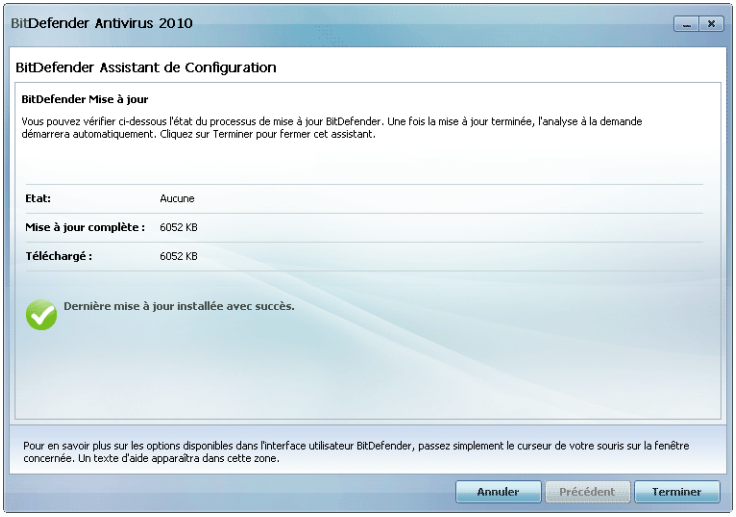
Si vous souhaitez changer l'heure de l'analyse par la suite, procédez comme suit :

1. Ouvrez BitDefender et faites passer l'interface utilisateur en Mode Expert.
2. Cliquez sur **Antivirus** dans le menu de gauche.
3. Cliquez sur l'onglet **Analyse antivirus**.
4. Faites un clic droit sur la tâche **Analyse du Système** et sélectionnez **Planifier**. Une nouvelle fenêtre s'affiche.
5. Modifiez la fréquence et l'heure de début comme vous le souhaitez.
6. Cliquez **OK** pour sauvegarder les changements.

Il est fortement recommandé d'activer ces options avant de passer à l'étape suivante pour assurer la sécurité de votre système. Cliquez sur **Suivant** pour continuer.

Si vous décochez la première case, il n'y a pas de tâches à réaliser lors de la dernière étape de l'assistant. Cliquez sur **Terminer** pour quitter l'assistant.

3.2.6. Étape 6 - Fin


BitDefender Antivirus 2010
BitDefender Assistant de Configuration
BitDefender Mise à jour
Vous pouvez vérifier ci-dessous l'état du processus de mise à jour BitDefender. Une fois la mise à jour terminée, l'analyse à la demande démarrera automatiquement. Cliquez sur Terminer pour fermer cet assistant.
Etat:
Aucune
Mise à jour complète :
6052 KB
Téléchargé :
6052 KB
Dernière mise à jour installée avec succès.
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Terminer

État d'avancement de la tâche

Attendez que BitDefender mette à jour ses signatures de codes malveillants et ses moteurs d'analyse. Dès que la mise à jour est terminée, une analyse rapide du système est lancée. L'analyse s'effectue en silence, en tâche de fond. Vous pouvez remarquer l'icône d'avancement de l'analyse dans la zone de notification. Vous pouvez cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

Cliquez sur **Terminer** pour quitter l'assistant. Vous n'avez pas besoin d'attendre que l'analyse soit terminée.

Note

L'analyse prend quelques minutes. Une fois terminée, ouvrez la fenêtre d'analyse et vérifiez les résultats de l'analyse pour voir si votre système est sain. Si des virus sont détectés pendant l'analyse, ouvrez BitDefender et lancez une analyse complète du système.

4. Mettre à niveau

Si vous utilisez BitDefender Antivirus 2010 bêta ou la version 2008 ou 2009, vous pouvez mettre à niveau vers BitDefender Antivirus 2010.

Il y a deux manières de réaliser la mise à niveau :

- Installez BitDefender Antivirus 2010 directement sur la version plus ancienne. Si vous installez votre produit directement par dessus une version 2009, les éléments en quarantaine seront automatiquement importés.
- Désinstallez la version la plus ancienne, puis redémarrez l'ordinateur et installez la nouvelle version comme expliqué dans le chapitre « *Installation de BitDefender* » (p. 5). Aucun paramètre du produit ne sera enregistré. Utilisez cette méthode de mise à niveau si l'autre échoue.

5. Réparer ou supprimer BitDefender

Si vous voulez réparer ou supprimer BitDefender Antivirus 2010, suivez ce chemin à partir du menu Démarrer de Windows : **Démarrer → Programmes → BitDefender 2010 → Réparer ou Supprimer**.

Il vous sera demandé confirmation de votre choix en cliquant sur **Suivant**. Une nouvelle fenêtre apparaîtra dans laquelle vous pourrez choisir:

- **Réparer** - pour réinstaller tous les composants choisis lors de l'installation précédente.

  Si vous décidez de réparer BitDefender, une nouvelle fenêtre s'affiche. Cliquez sur **Réparer** pour lancer le processus.

  Redémarrez l'ordinateur lorsque cela vous sera démandé puis cliquez sur **Installer** pour réinstaller BitDefender Antivirus 2010.

  Une fois l'installation achevée, une nouvelle fenêtre s'affiche. Cliquez sur **Terminer**.

- **Supprimer** - pour supprimer tous les composants installés.

  Note

  Nous vous recommandons de sélectionner **Supprimer** pour que la réinstallation soit saine.

  Si vous décidez de supprimer BitDefender, une nouvelle fenêtre s'affiche.

  Important

  Uniquement Windows Vista ! Si vous supprimez BitDefender, votre ordinateur ne sera plus protégé contre les menaces de malwares, tels que les virus et les spywares. Si vous souhaitez activer Windows Defender une fois BitDefender désinstallé, cochez la case correspondante.

  Cliquez sur **Supprimer** pour désinstaller BitDefender Antivirus 2010 de votre ordinateur.

  Une fois la désinstallation achevée, une nouvelle fenêtre s'affiche. Cliquez sur **Terminer**.

  Note

  A l'issue de la désinstallation, nous vous recommandons de supprimer le sous-dossier `BitDefender` du dossier `Program Files`.

Pour démarrer

6. Présentation

Une fois BitDefender installé, votre ordinateur est protégé. Si vous n'avez pas terminé l'assistant de configuration, ouvrez BitDefender dès que possible et corrigez les problèmes rencontrés. Vous pouvez avoir à configurer des composants BitDefender spécifiques ou appliquer des actions préventives afin de protéger votre ordinateur et vos données. Si vous le souhaitez, vous pouvez configurer BitDefender de sorte qu'il ne vous alerte pas au sujet de problèmes spécifiques.

Si vous n'avez pas enregistré le produit (y compris si vous n'avez pas créé de compte BitDefender), pensez à le faire avant que ne se termine la période d'essai. Vous devez créer un compte dans les 15 jours après l'installation de BitDefender (si vous l'enregistrez avec une clé de licence, l'expiration est repoussée à 30 jours). Dans le cas contraire, BitDefender ne se mettra plus à jour. Pour plus d'informations sur le processus d'enregistrement, veuillez vous référer à « *Enregistrement et Mon compte* » (p. 50).

6.1. Ouverture de BitDefender

Pour accéder à l'interface principale de BitDefender Antivirus 2010, cliquez dans le menu Démarrer de Windows sur **Démarrer → Programmes → BitDefender 2010 → BitDefender Antivirus 2010** ou double-cliquez directement sur l'icône BitDefender de la zone de notification.

6.2. Modes d'affichage de l'interface utilisateur

BitDefender Antivirus 2010 répond aux besoins de tous les utilisateurs, qu'ils soient débutants ou armés de solides connaissances techniques. Son interface utilisateur graphique est conçue pour s'adapter à chaque catégorie d'utilisateurs.

Vous pouvez choisir d'afficher l'interface utilisateur avec l'un des trois modes, en fonction de vos compétences en informatique et de votre connaissance de BitDefender.

Mode	Description
Mode Débutant	Convient aux débutants en informatique et aux personnes qui souhaitent que BitDefender protège leur ordinateur et leurs données sans être interrompues. Ce mode est facile à utiliser et ne requiert de votre part que très peu d'interventions. Vous devez simplement corriger les problèmes rencontrés comme indiqué par BitDefender. Un assistant intuitif vous guidera pas à pas dans la résolution de ces problèmes. Vous pouvez également

Mode	Description
	réaliser des tâches courantes comme la mise à jour des signatures de virus BitDefender et des fichiers du programme ou l'analyse de l'ordinateur.
Mode Intermédiaire	Conçu pour des utilisateurs ayant des compétences moyennes en informatique, ce mode étend les possibilités du Mode Débutant. Vous pouvez corriger les problèmes séparément et choisir les éléments à surveiller. De plus, vous pouvez gérer à distance les produits BitDefender installés sur les ordinateurs de votre foyer.
Mode Expert	Ce mode, qui convient à des utilisateurs ayant plus de connaissances techniques, vous permet de configurer en détail chaque fonctionnalité de BitDefender. Vous pouvez également utiliser toutes les tâches fournies pour protéger votre ordinateur et vos données.

Le mode de l'interface utilisateur est sélectionné dans l'assistant de configuration. L'assistant apparaît après l'assistant d'enregistrement, la première fois que vous allumez votre ordinateur après avoir installé le produit. Si vous annulez l'assistant de configuration, le mode Intermédiaire s'appliquera par défaut à l'interface utilisateur.

Pour modifier le mode de l'interface utilisateur, suivez ces étapes :

1. Lancer BitDefender.
2. Cliquez sur le bouton **Configuration** dans l'angle supérieur droit de la fenêtre.
3. Dans la catégorie Configuration de l'Interface Utilisateur, cliquez sur la flèche du bouton et sélectionnez le mode souhaité à partir du menu.
4. Cliquez sur **OK** pour enregistrer et appliquer les modifications.

6.2.1. Mode Débutant

Si vous êtes débutant en informatique, afficher l'interface utilisateur en Mode Débutant peut être le choix vous convenant le mieux. Ce mode est simple à utiliser et ne requiert que très peu d'interventions de votre part.

BitDefender Antivirus 2010-Version d'évaluation
Configuration
État de sécurité
ATTENTION : 5 problèmes affectent l'état de sécurité de ce PC.
Tout corriger
Besoin d'aide ?
Protéger Votre PC
Analyser
Mettre à jour
Vulnérabilités
Outils supplémentaires
Cliquez pour développer
Type de profil : Personnalisé
Pour en savoir plus sur les options disponibles dans l'interface utilisateur, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
bitdefender
Acheter S'enregistrer Support Votre avis Aide Journaux

Mode Débutant

La fenêtre est constituée de quatre sections principales :

- L'**État de Sécurité** vous avertit si des problèmes affectent la sécurité de votre ordinateur et vous aide à les corriger. Si vous cliquez sur **Corriger tous les problèmes**, un assistant vous aidera à supprimer facilement toutes les menaces affectant votre ordinateur et la sécurité de vos données. Pour plus d'informations, reportez-vous à « *Correction des problèmes* » (p. 38).
- **Protéger Votre PC** est l'endroit où vous pouvez trouver les tâches nécessaires à la protection de votre ordinateur et de vos données. Les tâches disponibles que vous pouvez réaliser sont différentes selon le profil d'utilisation sélectionné.
  - Le bouton **Analyser** lance une analyse standard de votre système et recherche la présence de virus, spywares et autres malwares. L'Assistant d'Analyse Antivirus apparaîtra et vous guidera tout au long du processus d'analyse. Pour plus d'informations sur cet assistant, veuillez consulter « *Assistant d'analyse antivirus* » (p. 55).
  - Le bouton **Mettre à jour** vous aide à mettre à jour les signatures de virus et les fichiers du produit BitDefender. Une nouvelle fenêtre apparaît affichant l'état de la mise à jour. Si des mises à jour sont détectées, elles sont automatiquement téléchargées et installées sur votre ordinateur.
  - Lorsque le profil **Standard** est sélectionné, le bouton **Contrôle de Vulnérabilités** lance un assistant qui vous aide à détecter et à corriger les vulnérabilités du système, comme des logiciels non à jour ou des mises à jour

Windows manquantes. Pour plus d'informations, reportez-vous à la section « *Assistant du Contrôle de Vulnérabilité* » (p. 67).

- Lorsque le profil **Gamer** est sélectionné, le bouton **Activer/Désactiver le Mode Jeu** vous permet d'activer/de désactiver le Mode Jeu. Le Mode Jeu modifie temporairement les paramètres de protection afin de minimiser leur impact sur les performances du système.

- **Entretenez Votre PC** est l'endroit où vous pouvez trouver des tâches supplémentaires pour protéger votre ordinateur et vos données.
  - **Analyse approfondie du système** lance une analyse complète de votre système pour rechercher tous les types de malwares.
  - **Analyse de Mes Documents** recherche la présence de virus et autres malwares dans les répertoires les plus souvent utilisés : `Mes Documents` et `Bureau`. Cela garantit la sécurité de vos documents, un espace de travail sûr et des applications s'exécutant au démarrage saines.
  - **Analyse automatique à l'ouverture de session** analyse les éléments qui s'exécutent lorsque vous vous connectez à Windows.
- **Profil Utilisateur** indique le profil utilisateur en cours d'utilisation. Le profil d'utilisation reflète les principales activités réalisées avec l'ordinateur. L'interface du produit s'adapte à votre profil d'utilisation pour vous permettre d'accéder facilement à vos tâches favorites.

  Si vous souhaitez changer de profil ou modifier celui que vous utilisez en ce moment, cliquez sur le profil et suivez l'assistant de configuration.

Dans l'angle supérieur droit de la fenêtre se trouve le bouton **Configuration**. Il ouvre une fenêtre où vous pouvez modifier le mode de l'interface utilisateur et activer ou désactiver les principaux paramètres de BitDefender. Pour plus d'informations, reportez-vous à « *Configuration des Paramètres de base* » (p. 42).

Dans l'angle inférieur droit de la fenêtre, vous trouverez plusieurs liens utiles.

Lien	Description
Acheter/Renouveler	Ouvre une page Web où vous pouvez acheter une clé de licence pour le produit BitDefender Antivirus 2010.
Enregistrement	Vous permet de saisir une nouvelle clé de licence ou de consulter la clé de licence actuelle et l'état de votre enregistrement.
Aide & Support	Vous donne accès à un fichier d'aide qui vous montrera comment utiliser BitDefender.

6.2.2. Mode Intermédiaire

Conçu pour des utilisateurs ayant des compétences informatiques moyennes, le Mode Intermédiaire est une interface simple qui vous donne accès à tous les modules à un niveau basique. Vous devrez prêter attention aux avertissements et aux alertes critiques et corriger les problèmes indésirables.

BitDefender Antivirus 2010 - Version d'évaluation
Configuration
TABLEAU DE BORD
ANTIVIRUS
ANTIPHISHING
VULNÉRABILITÉS
RÉSEAU
État de sécurité
Profil d'utilisation: Personnalisé
Mettre à jour
ATTENTION : 5 problèmes affectent l'état de sécurité de ce PC.
Tout corriger
Détails
ANTIVIRUS
ALERTE CRITIQUE - 1 problème en attente
ANTIPHISHING
PROTÉGÉ - Aucun problème
VULNÉRABILITÉS
ALERTE CRITIQUE - 4 problèmes en attente
RÉSEAU
ALERTE CRITIQUE - Des problèmes de sécurité affectent les ordinateurs de votre réseau
Le module Tableau de bord affiche l'état de sécurité du produit ainsi que des liens vers les principaux modules du produit.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

Mode Intermédiaire

La fenêtre du Mode Intermédiaire se compose de cinq onglets. Le tableau suivant décrit brièvement chaque onglet. Pour plus d'informations, veuillez vous référer à la partie « Mode Intermédiaire » (p. 74) de ce guide d'utilisation.

Onglet	Description
Tableau de bord	Affiche l'état de sécurité de votre système et vous permet de réinitialiser le profil d'utilisation.
Antivirus	Affiche l'état du module antivirus qui vous aide à maintenir votre antivirus à jour et vous protège des virus.
Antiphishing	Affiche l'état des modules qui vous protègent contre le phishing (vol d'informations personnelles) lorsque vous êtes en ligne.
Vulnérabilité	Affiche l'état du module d'analyse des vulnérabilités qui vous aide à maintenir à jour les logiciels majeurs de votre ordinateur. Vous pouvez facilement corriger ici toute

Onglet	Description
	vulnérabilité susceptible d'affecter la sécurité de votre ordinateur.
Réseau	Affiche la structure du réseau domestique BitDefender. Vous pouvez effectuer ici plusieurs actions pour configurer et gérer les produits BitDefender installés sur votre réseau domestique. De cette façon, vous pouvez gérer la sécurité de votre réseau domestique à partir d'un seul ordinateur.

Dans l'angle supérieur droit de la fenêtre se trouve le bouton **Configuration**. Il ouvre une fenêtre où vous pouvez modifier le mode de l'interface utilisateur et activer ou désactiver les principaux paramètres de BitDefender. Pour plus d'informations, reportez-vous à « *Configuration des Paramètres de base* » (p. 42).

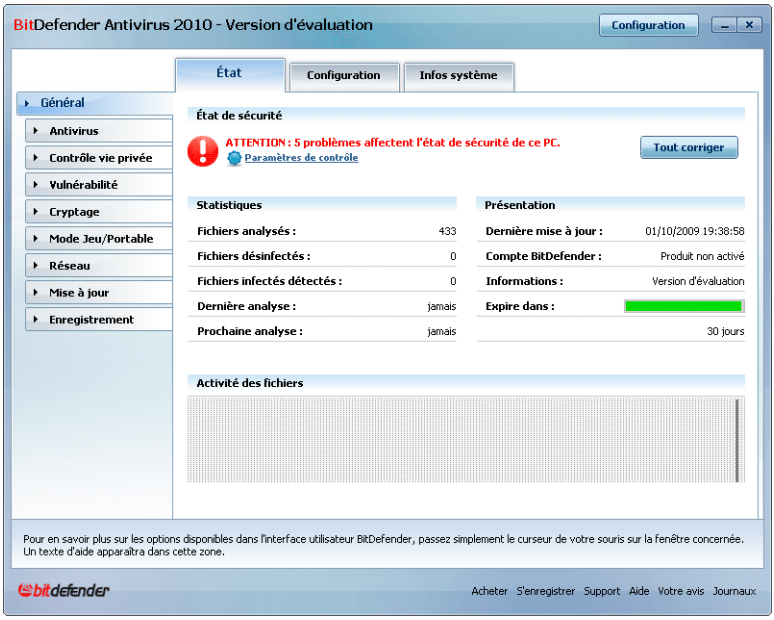
Dans l'angle inférieur droit de la fenêtre, vous trouverez plusieurs liens utiles.

Lien	Description
Acheter/Renouveler	Ouvre une page Web où vous pouvez acheter une clé de licence pour le produit BitDefender Antivirus 2010.
Enregistrer	Vous permet de saisir une nouvelle clé de licence ou de consulter la clé de licence actuelle et l'état de votre enregistrement.
Support	Vous permet de contacter l'équipe du Support Technique BitDefender.
Aide	Vous donne accès à un fichier d'aide qui vous montrera comment utiliser BitDefender.
Afficher les Journaux	Vous permet d'afficher un historique détaillé de toutes les tâches exécutées par BitDefender sur votre système.

6.2.3. Mode Expert

Le Mode Expert vous donne accès à chaque composant de BitDefender. Vous pouvez y configurer BitDefender en détail.

Note
Le Mode Expert convient aux utilisateurs ayant des compétences en informatique supérieures à la moyenne, qui connaissent les types d'e-menaces auxquels un ordinateur est exposé et qui savent comment fonctionnent les programmes de sécurité.



Mode Expert

À gauche de la fenêtre figure un menu contenant l'intégralité des modules de sécurité. Chaque module comprend un ou plusieurs onglet(s) où vous pouvez configurer les paramètres de sécurité correspondants, et effectuer des actions de sécurité ou des tâches administratives. Le tableau suivant décrit brièvement chaque module. Pour plus d'informations, veuillez vous référer à la partie « Mode Expert » (p. 96) de ce guide d'utilisation.

Module	Description
Général	Vous permet d'accéder aux paramètres généraux ou de consulter le tableau de bord et des informations détaillées sur le système.
Antivirus	Vous permet de configurer en détail votre antivirus et les opérations d'analyse, de définir les exceptions et de configurer le module Quarantaine.
Contrôle Vie privée	Vous permet d'éviter le vol de données sur votre ordinateur et de protéger votre vie privée lorsque vous êtes en ligne.

Module	Description
Vulnerabilité	Vous permet de maintenir à jour les logiciels majeurs de votre ordinateur.
Cryptage	Vous permet de crypter les communications Yahoo et Windows Live (MSN) Messenger.
Mode Jeu/Portable	Vous permet de reporter les tâches BitDefender programmées si votre ordinateur portable fonctionne sur batterie, ainsi que de désactiver toutes les alertes et pop-up lorsqu'un jeu vidéo est lancé.
Réseau	Vous permet de configurer et de gérer les différents ordinateurs présents dans votre foyer.
Mise à jour	Vous permet d'obtenir des informations sur les dernières mises à jour, de mettre à jour votre produit et de configurer en détail le processus de mise à jour.
Enregistrement	Vous permet d'enregistrer BitDefender Antivirus 2010, de modifier la clé de licence ou de créer un compte BitDefender.

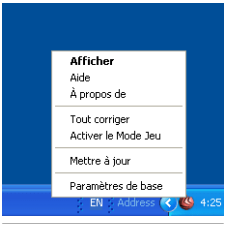
Dans l'angle supérieur droit de la fenêtre se trouve le bouton **Configuration**. Il ouvre une fenêtre où vous pouvez modifier le mode de l'interface utilisateur et activer ou désactiver les principaux paramètres de BitDefender. Pour plus d'informations, reportez-vous à « *Configuration des Paramètres de base* » (p. 42).

Dans l'angle inférieur droit de la fenêtre, vous trouverez plusieurs liens utiles.

Lien	Description
Acheter/Renouveler	Ouvre une page Web où vous pouvez acheter une clé de licence pour le produit BitDefender Antivirus 2010.
Enregistrer	Vous permet de saisir une nouvelle clé de licence ou de consulter la clé de licence actuelle et l'état de votre enregistrement.
Support	Vous permet de contacter l'équipe du Support Technique BitDefender.
Aide	Vous donne accès à un fichier d'aide qui vous montrera comment utiliser BitDefender.
Afficher les Journaux	Vous permet d'afficher un historique détaillé de toutes les tâches exécutées par BitDefender sur votre système.

6.3. Icône de la zone de notification

Pour gérer l'ensemble du produit plus rapidement, vous pouvez utiliser l'icône BitDefender de la zone de notification. Double-cliquez sur cette icône pour ouvrir BitDefender. Si vous effectuez un clic droit sur cette icône, le menu contextuel qui apparaît vous permettra de gérer le produit BitDefender plus rapidement.



Icône

- **Afficher** - ouvre l'interface principale BitDefender.
- **Aide** - ouvre le fichier d'aide, qui explique en détail comment configurer et utiliser BitDefender Antivirus 2010.
- **A propos de** - Affichage d'une fenêtre contenant des informations relatives à BitDefender, ainsi que des éléments d'aide si vous rencontrez une situation anormale.
- **Corriger tous les problèmes** - vous aide à résoudre les problèmes de vulnérabilité de votre ordinateur en matière de sécurité. Si l'option n'est pas disponible, c'est qu'il n'y a pas de problème à corriger. Pour plus d'informations, reportez-vous à « *Correction des problèmes* » (p. 38).
- **Activer / désactiver le Mode Jeu** - active / désactive le Mode Jeu.
- **Mettre à jour** - effectue une mise à jour immédiate. Une nouvelle fenêtre apparaît affichant l'état de la mise à jour.
- **Paramètres de base** - ouvre une fenêtre où vous pouvez modifier le mode de l'interface utilisateur et activer ou désactiver les principaux paramètres du produit. Pour plus d'informations, reportez-vous à « *Configuration des Paramètres de base* » (p. 42).

L'icône de la zone de notification de BitDefender vous informe de la présence de problèmes affectant la sécurité de votre ordinateur et du fonctionnement du programme en affichant un symbole spécial :

Triangle rouge avec un point d'exclamation : D'importants problèmes affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.

Triangle jaune avec un point d'exclamation : Des problèmes non critiques affectent la sécurité de votre système. Vérifiez-les et réglez-les lorsque vous aurez le temps.

Lettre G: Le produit fonctionne en Mode jeu.

Si BitDefender ne fonctionne pas, l'icône de la zone de notification est grisée. Cela se produit généralement lorsque la clé de licence expire. Cela peut également avoir lieu lorsque les services BitDefender ne répondent pas ou lorsque d'autres erreurs affectent le fonctionnement normal de BitDefender.

6.4. Barre de l'activité d'analyse

La **Barre d'analyse d'activité** est une visualisation graphique de l'analyse d'activité de votre système. Cette petite fenêtre est disponible par défaut uniquement dans le Mode Expert.

Les barres grises (la **Fichiers**) montrent le nombre de fichiers analysés par seconde, sur une échelle de 0 à 50.

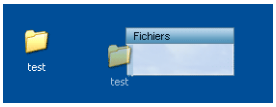
Barre de l'activité d'analyse

Note
La barre d'analyse d'activité vous prévient lorsque la protection en temps réel est désactivée en affichant une croix rouge au-dessus du **fichier**.

6.4.1. Analyser Fichiers et Dossiers

Vous pouvez utiliser la barre d'activité d'analyse pour analyser rapidement des fichiers et des dossiers. Glissez le fichier ou répertoire que vous voulez analyser et déposez-le sur la **Barre d'analyse de l'activité**, comme sur l'image ci-dessous.

Glisser le fichier



Déposer le fichier

L'Assistant d'Analyse Antivirus apparaîtra et vous guidera tout au long du processus d'analyse. Pour plus d'informations sur cet assistant, veuillez consulter « *Assistant d'analyse antivirus* » (p. 55).

Options d'analyse. Les options d'analyse sont déjà configurées pour que la détection soit la meilleure possible. Si des fichiers infectés sont détectés, BitDefender essaiera de les désinfecter (suppression du code du malware). Si la désinfection échoue, l'assistant d'analyse antivirus vous proposera d'indiquer d'autres moyens d'intervenir sur les fichiers infectés. Les options d'analyse sont standard et vous ne pouvez pas les modifier.

6.4.2. Désactiver/Restaurer la Barre d'Activité d'Analyse

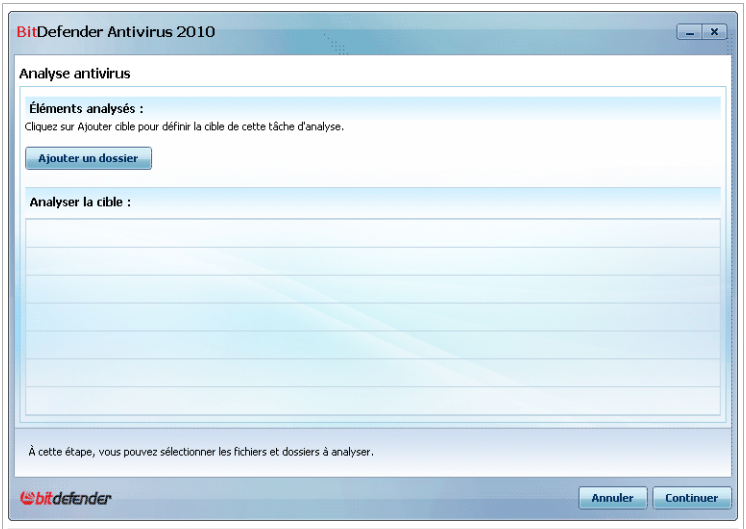
Si vous ne souhaitez plus voir cette barre, il vous suffit de faire un clic-droit dessus et de choisir **Cacher**. Pour restaurer la barre d'activité d'analyse, suivez ces étapes :

1. Lancer BitDefender.
2. Cliquez sur le bouton **Configuration** dans l'angle supérieur droit de la fenêtre.
3. Dans la catégorie Paramètres Généraux, cochez la case correspondant à **Barre d'activité d'analyse** .
4. Cliquez sur **OK** pour enregistrer et appliquer les modifications.

6.5. Analyse Manuelle BitDefender

BitDefender Manual Scan vous permet d'analyser un dossier particulier ou une partition d'un disque dur sans avoir à créer une tâche d'analyse. Cette fonctionnalité est conçue pour être utilisée lorsque Windows a été démarré en Mode sans échec Si votre système est infecté par un virus résistant, vous pouvez essayer de le supprimer en faisant démarrer Windows en Mode sans échec et en faisant analyser chaque partition du disque par BitDefender Manual Scan.

Pour accéder à l'Analyse manuelle BitDefender, cliquez dans le menu Démarrer de Windows sur **Démarrer → Programmes → BitDefender 2010 → Analyse Manuelle BitDefender**. La fenêtre suivante apparaît:


BitDefender Antivirus 2010
Analyse antivirus
Éléments analysés :
Cliquez sur Ajouter cible pour définir la cible de cette tâche d'analyse.
Ajouter un dossier
Analyser la cible :
À cette étape, vous pouvez sélectionner les fichiers et dossiers à analyser.
bitdefender
Annuler
Continuer

Analyse Manuelle BitDefender

Cliquez sur **Ajouter Dossier**, sélectionnez l'emplacement que vous voulez analyser et cliquez sur **OK**. Si vous voulez analyser plusieurs dossiers, répétez cette action pour chaque emplacement supplémentaire.

Les chemins vers les emplacements sélectionnés apparaîtront dans la colonne **Cible de l'Analyse**. Si vous changez d'avis pour un emplacement donné, cliquez simplement sur le bouton **Supprimer** situé en regard de l'emplacement. Cliquez sur le bouton **Supprimer tous les chemins** pour supprimer tous les emplacements qui avaient été ajoutés à la liste.

Une fois les emplacements sélectionnés, cliquez sur **Continuer**. L'Assistant d'Analyse Antivirus apparaîtra et vous guidera tout au long du processus d'analyse. Pour plus d'informations sur cet assistant, veuillez consulter « *Assistant d'analyse antivirus* » (p. 55).

Options d'analyse. Les options d'analyse sont déjà configurées pour que la détection soit la meilleure possible. Si des fichiers infectés sont détectés, BitDefender essaiera de les désinfecter (suppression du code du malware). Si la désinfection échoue, l'assistant d'analyse antivirus vous proposera d'indiquer d'autres moyens d'intervenir sur les fichiers infectés. Les options d'analyse sont standard et vous ne pouvez pas les modifier.

Que signifie Mode sans échec ?
Le Mode sans échec est une façon particulière de démarrer Windows, principalement utilisée pour localiser les problèmes liés au fonctionnement normal de Windows. De tels problèmes peuvent provenir d'un conflit entre pilotes ou de virus empêchant Windows de démarrer normalement. En Mode sans échec, Windows ne charge qu'un minimum de composants du système d'exploitation et les pilotes de base. Il n'existe que quelques applications qui fonctionnent en Mode sans échec. C'est pour cette raison que la plupart des virus sont inactifs et peuvent être facilement supprimés quand Windows est utilisé dans ce mode.
Pour faire démarrer Windows en Mode sans échec, redémarrez votre ordinateur et appuyez sur la touche F8 jusqu'à ce que le menu des fonctions avancées de Windows s'affiche. Vous pouvez choisir entre plusieurs options de démarrage de Windows en Mode sans échec. Vous pourrez sélectionner **Mode sans échec avec réseau** si vous souhaitez pouvoir accéder à Internet.

Note

Pour plus d'informations sur le Mode sans échec, allez dans le centre d'aide et de support de Windows (dans le menu Démarrer, cliquez sur **Aide et support**). Vous pouvez également rechercher des informations sur Internet.

6.6. Mode Jeu et Mode Portable

Certaines utilisations de l'ordinateur, comme les jeux ou les présentations, nécessitent plus de performance et de réactivité du système, et aucune interruption. Lorsque votre ordinateur portable est alimenté par sa batterie, il vaut mieux que

les opérations non indispensables, qui consomment de l'énergie supplémentaire, soient reportées jusqu'au moment où l'ordinateur portable sera branché sur secteur.

Pour s'adapter à ces situations particulières, BitDefender Antivirus 2010 comprend deux modes de fonctionnement spéciaux :

- Mode Jeu
- Mode Portable

6.6.1. Mode Jeu

Le Mode Jeu modifie temporairement les paramètres de protection afin de minimiser leur impact sur les performances du système. Les paramètres suivants sont appliqués lorsque vous êtes en Mode Jeu :

- Réduire les sollicitations processeur et la consommation de mémoire
- Reporter les mises à jour automatiques et les analyses
- Éliminer toutes les alertes et pop-up
- Analyser uniquement les fichiers les plus importants

Lorsque vous êtes en Mode Jeu, vous pouvez voir la lettre G incrustée sur l'icône BitDefender.

Utilisation du Mode Jeu

Par défaut, BitDefender passe automatiquement en Mode Jeu lorsque vous lancez un jeu figurant dans la liste des jeux connus de BitDefender, ou lorsqu'une application s'exécute en mode plein écran. BitDefender reprendra automatiquement le mode de fonctionnement normal lorsque vous fermerez le jeu ou lorsque l'application détectée quittera le mode plein écran.

Si vous souhaitez activer manuellement le Mode Jeu, utilisez l'une des méthodes suivantes :

- Faites un Clic-droit sur l'icône BitDefender dans la barre d'état et sélectionnez **Activer le Mode Jeu**.
- Appuyez sur les touches `Ctrl+Shift+Alt+G` (le raccourci clavier par défaut).

Important
N'oubliez pas de désactiver le Mode Jeu lorsque vous aurez fini. Pour cela, utilisez les mêmes méthodes que celles utilisées pour l'activer.

Changer le raccoruci clavier du Mode Jeu

Pour changer le raccourci clavier, suivez ces étapes :

1. Ouvrez BitDefender et faites passer l'interface utilisateur en Mode Expert.
2. Cliquez sur **Mode Jeu / Portable** dans le menu de gauche.

3. Cliquez sur l'onglet **Mode Jeu**.
4. Cliquez sur **Paramètres avancés**.
5. Sous l'option **Utiliser le raccourci**, définissez le raccourci clavier désiré :
   - Choisissez la touche que vous souhaitez utiliser en cochant l'une des suivantes : touche Contrôle (`Ctrl`), Touche Shift(`Shift`) ou touche Alt (`Alt`).
   - Dans le champ éditable, entrez la lettre que vous souhaitez utiliser.

   Par exemple, si vous souhaitez utiliser le raccourci `Ctrl+Alt+D`, vous devez cocher seulement `Ctrl` et `Alt` et tapez `D`.

   Note
   En décochant la case **Utiliser le raccourci**, vous désactivez le raccourci clavier.

6. Cliquez **OK** pour sauvegarder les changements.

6.6.2. Mode Portable

Le Mode Portable est spécialement conçu pour les utilisateurs d'ordinateurs portables et de notebooks. Son objectif est de minimiser l'impact de BitDefender sur la consommation d'énergie lorsque ces périphériques sont alimentés par leur batterie. En Mode Portable, les tâches d'analyse planifiées ne sont pas effectuées car elles nécessitent plus de ressources système et donc, réduisent l'autonomie de la batterie.

BitDefender détecte le passage d'une alimentation secteur à une alimentation sur batterie et passe automatiquement en Mode Portable. De la même manière, BitDefender quitte automatiquement le Mode Portable lorsqu'il détecte que l'ordinateur portable ne fonctionne plus sur batterie.

Pour utiliser le Mode Portable, vous devez indiquer dans l'assistant de configuration que vous utilisez un ordinateur portable. Si vous n'avez pas sélectionné l'option appropriée lors de l'exécution de l'assistant, vous pouvez activer le Mode Portable par la suite comme indiqué :

1. Lancer BitDefender.
2. Cliquez sur le bouton **Configuration** dans l'angle supérieur droit de la fenêtre.
3. Dans la catégorie Paramètres Généraux, cochez la case correspondant à **Détection du Mode Portable**.
4. Cliquez sur **OK** pour enregistrer et appliquer les modifications.

6.7. Détection automatique de périphérique

BitDefender détecte automatiquement la connexion d'un périphérique de stockage amovible à votre ordinateur et vous propose de l'analyser avant que vous accédiez

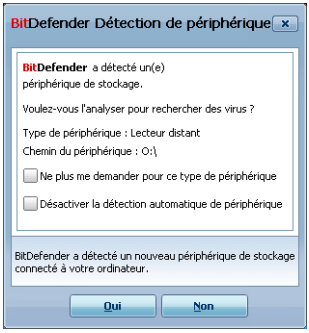
à ses fichiers. Ceci est recommandé afin d'empêcher que des virus ou autres malwares n'infectent votre ordinateur.

Les périphériques détectés appartiennent à l'une des catégories suivantes :

- CD/DVD
- Des mémoires USB, tels que des clés flash et des disques durs externes
- disques réseau (distants) connectés

Lorsqu'un tel périphérique est détecté, une fenêtre d'alerte s'affiche.

Pour analyser le périphérique de stockage, cliquez simplement sur **Oui**. L'Assistant d'Analyse Antivirus apparaîtra et vous guidera tout au long du processus d'analyse. Pour plus d'informations sur cet assistant, veuillez consulter « *Assistant d'analyse antivirus* » (p. 55).


BitDefender Détection de périphérique
BitDefender a détecté un(e) périphérique de stockage.
Voulez-vous l'analyser pour rechercher des virus ?
Type de périphérique : Lecteur distant
Chemin du périphérique : O:\
Ne plus me demander pour ce type de périphérique
Désactiver la détection automatique de périphérique
BitDefender a détecté un nouveau périphérique de stockage connecté à votre ordinateur.
Oui
Non
Détection de périphérique

Si vous ne souhaitez pas analyser le périphérique, cliquez sur **Non**. Dans ce cas, il se peut que l'une des options suivantes vous semble utile :

- **Ne plus me demander pour ce type de périphérique** - BitDefender ne proposera plus d'analyser ce type de périphériques de stockage lorsqu'ils seront connectés à votre ordinateur.
- **Désactiver la détection automatique de périphérique** - On ne vous proposera plus d'analyser les nouveaux périphériques de stockage lorsqu'ils seront connectés à l'ordinateur.

Si vous avez désactivé par erreur la détection automatique de périphérique et que vous voulez l'activer, ou si vous souhaitez configurer ses paramètres, procédez comme suit :

1. Ouvrez BitDefender et faites passer l'interface utilisateur en Mode Expert.
2. Allez dans **Antivirus>Analyse Antivirus**.
3. Dans la liste des tâches d'analyse, localisez la tâche **Analyse des périphériques détectés**.
4. Faites un clic droit sur la tâche et sélectionnez **Ouvrir**. Une nouvelle fenêtre s'affiche.
5. Dans l'onglet **Présentation**, configurez les options d'analyse selon vos besoins. Pour plus d'informations veuillez vous reporter à « *Configuration des paramètres d'analyse* » (p. 121).
6. Dans l'onglet **Détection**, sélectionnez les types de périphériques de stockage à détecter.
7. Cliquez sur **OK** pour enregistrer et appliquer les modifications.

7. Correction des problèmes

BitDefender utilise un système de contrôle pour détecter la présence de problèmes pouvant affecter la sécurité de votre ordinateur et de vos données et vous en informer. Par défaut, il surveille seulement un ensemble de problèmes considérés comme très importants. Cependant, vous pouvez le configurer selon vos besoins en sélectionnant les problèmes spécifiques au sujet desquels vous souhaitez être averti(e).

Voici comment les problèmes en attente sont signalés :

- Un symbole spécial apparaît sur l'icône de BitDefender dans la zone de notification pour signaler la présence de problèmes en attente.

  Triangle rouge avec un point d'exclamation : D'importants problèmes affectent la sécurité de votre système. Ils requièrent votre attention immédiate et doivent être réglés dès que possible.
  Triangle jaune avec un point d'exclamation : Des problèmes non critiques affectent la sécurité de votre système. Vérifiez-les et réglez-les lorsque vous aurez le temps.

  Si vous passez le curseur de la souris sur l'icône, une fenêtre de notification confirmera la présence de problèmes en attente.

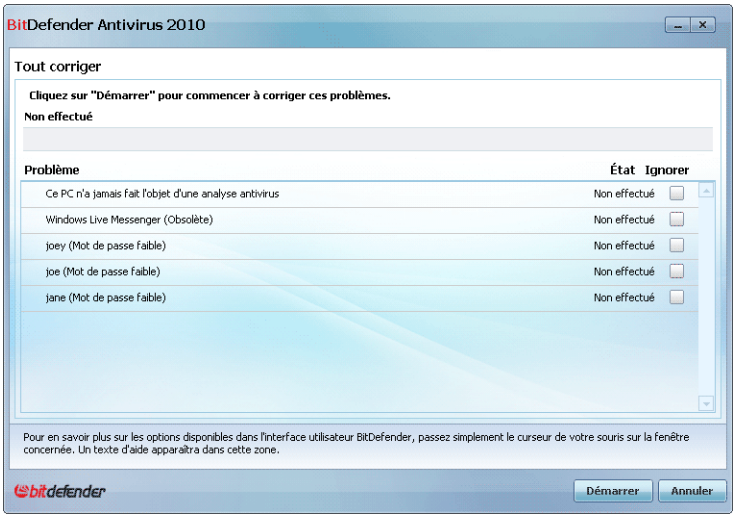
- Lorsque vous ouvrez BitDefender, la zone d'État de Sécurité indique le nombre de problèmes affectant votre système.
  - En Mode Intermédiaire, l'état de sécurité apparaît dans l'onglet **Tableau de bord**
  - En Mode Expert, allez dans **Général > Tableau de bord** pour vérifier l'état de sécurité.

7.1. Assistant de Correction des Problèmes

La manière la plus simple de corriger les problèmes existants est de suivre pas à pas l'assistant de **Correction des Problèmes**. L'assistant vous aide à supprimer facilement les menaces affectant votre ordinateur et la sécurité de vos données. Pour ouvrir l'assistant, procédez comme indiqué :

- Faites un clic droit sur l'icône de BitDefender dans la zone de notification et sélectionnez **Corriger tous les problèmes**.
- Lancer BitDefender. En fonction du mode de l'interface utilisateur, procédez comme suit :
  - En Mode Débutant, cliquez sur **Corriger tous les problèmes**.
  - En Mode Intermédiaire, allez dans l'onglet **Tableau de bord** et cliquez sur **Corriger tous les problèmes**.

▶ En Mode Expert, allez dans **Général>Tableau de bord** et cliquez sur **Corriger tous les problèmes**.


BitDefender Antivirus 2010
Tout corriger
Cliquez sur "Démarrer" pour commencer à corriger ces problèmes.
Non effectué
Problème
État
Ignorer
Ce PC n'a jamais fait l'objet d'une analyse antivirus
Non effectué
Windows Live Messenger (Obsolète)
Non effectué
joey (Mot de passe faible)
Non effectué
joe (Mot de passe faible)
Non effectué
jane (Mot de passe faible)
Non effectué
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
bitdefender
Démarrer
Annuler

Assistant de Correction des Problèmes

L'assistant affiche la liste des failles de sécurité présentes sur votre ordinateur.

Tous les problèmes présents sont sélectionnés pour être corrigés. Si vous ne voulez pas corriger un problème, cochez simplement la case correspondante. Son état passera alors à **Ignorer**.

Note
Si vous ne voulez pas être informé(e) de la présence de certains problèmes, vous devez configurer le système de contrôle en conséquence, comme décrit dans la section suivante.

Pour corriger les problèmes sélectionnés, cliquez sur **Démarrer**. Certains problèmes sont corrigés immédiatement. Pour d'autres, un assistant vous aide à les corriger.

Les problèmes que cet assistant vous aide à corriger peuvent être regroupés dans les catégories suivantes :

- **Paramètres de sécurité désactivés.** Ces problèmes sont corrigés immédiatement en activant les paramètres de sécurité correspondants.
- **Tâches de sécurité préventives que vous avez besoin de réaliser.** Un exemple de ce type de tâches est l'analyse de votre ordinateur. Nous vous recommandons d'analyser votre ordinateur au moins une fois par semaine. En

général, BitDefender réalisera cette analyse pour vous de façon automatique. Mais si vous avez modifié la planification de l'analyse ou si la planification n'a pas été réalisée, ce problème vous sera signalé.

Un assistant vous aide à corriger ces problèmes.

- **Vulnérabilités du Système.** BitDefender recherche automatiquement les vulnérabilités de votre système et vous les signale. Les vulnérabilités du Système peuvent être :
  - des mots de passe non sécurisés de comptes utilisateurs Windows
  - la présence sur votre ordinateur de logiciels non à jour
  - des mises à jour Windows manquantes
  - les mises à jour automatiques de Windows sont désactivées

  Lorsque de tels problèmes doivent être corrigés, l'assistant de l'analyse de vulnérabilité est lancé. Cet assistant vous aide à corriger les vulnérabilités du système qui ont été détectées. Pour plus d'informations, reportez-vous à la section « *Assistant du Contrôle de Vulnérabilité* » (p. 67).

7.2. Configuration du système de contrôle

Le système de contrôle est pré-configuré pour surveiller les problèmes pouvant affecter la sécurité de votre ordinateur et de vos données et vous signaler les principaux. D'autres problèmes peuvent être surveillés en fonction des choix que vous faites dans l'assistant de configuration (lorsque vous configurez votre profil d'utilisation). Outre les problèmes surveillés par défaut, plusieurs autres problèmes peuvent vous être signalés.

Vous pouvez configurer le système de contrôle afin qu'il réponde mieux à vos besoins en sécurité en choisissant les problèmes que vous souhaitez que l'on vous signale. Vous pouvez faire cela en Mode Intermédiaire ou en Mode Expert.

- En Mode Intermédiaire, le système de contrôle peut être configuré à partir de différents endroits. Suivez ces étapes :
  1. Allez dans l'onglet **Antivirus**, **Antiphishing** ou **Vulnérabilité**.
  2. Cliquez sur **Configurer le système de contrôle d'état**.
  3. Cochez les cases correspondant aux éléments que vous souhaitez surveiller.

  Pour plus d'informations, veuillez vous référer à la partie « Mode Intermédiaire » (p. 74) de ce guide d'utilisation.

- En Mode Expert, le système de contrôle peut être configuré à partir d'un emplacement central. Suivez ces étapes :
  1. Allez dans **Général>Tableau de bord**.
  2. Cliquez sur **Configurer le système de contrôle d'état**.
  3. Cochez les cases correspondant aux éléments que vous souhaitez surveiller.

Pour plus d'informations, reportez-vous au chapitre « *État* » (p. 97).

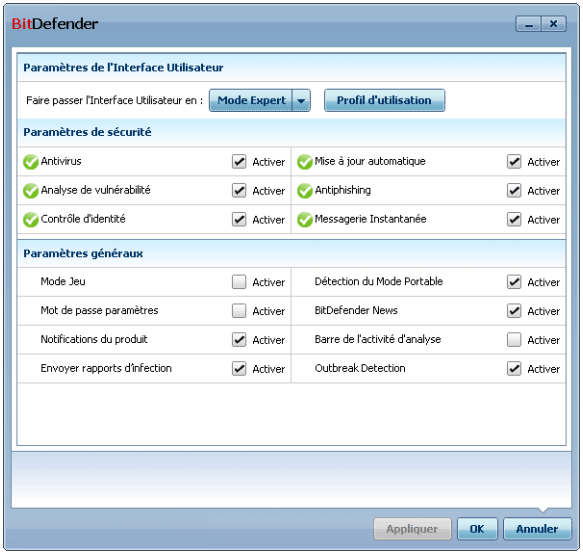
8. Configuration des Paramètres de base

Vous pouvez configurer les principaux paramètres du produit (y compris changer le mode d'affichage de l'interface utilisateur) à partir de la fenêtre paramètres de base. Pour l'ouvrir, utilisez l'une des méthodes suivantes :

- Ouvrez BitDefender et cliquez sur le bouton **Paramètres** dans l'angle supérieur droit de la fenêtre.
- Faites un clic droit sur l'icône BitDefender dans la zone de notification et sélectionnez **Paramètres de base**.

Note

Pour configurer les paramètres du produit en détail, utilisez le Mode Expert de l'interface. Pour plus d'informations, veuillez vous référer à la partie « Mode Expert » (p. 96) de ce guide d'utilisation.



Paramètres de base

Les paramètres sont regroupés en trois catégories :

- Paramètres de l'Interface Utilisateur
- Paramètres de Sécurité
- Paramètres Généraux

Pour appliquer et enregistrer les modifications de configuration que vous faites, cliquez sur **OK**. Pour fermer la fenêtre sans enregistrer les modifications, cliquez sur **Annuler**.

8.1. Paramètres de l'Interface Utilisateur

Dans cette zone, vous pouvez changer le mode d'affichage de l'interface utilisateur et réinitialiser le profil d'utilisation.

Changer le mode d'affichage de l'interface utilisateur. Comme décrit dans la section « *Modes d'affichage de l'interface utilisateur* » (p. 23), il existe trois modes d'affichage de l'interface utilisateur. Chaque mode de l'interface utilisateur est conçu pour une catégorie spécifique d'utilisateurs, en fonction de leurs compétences en informatique. De cette façon, l'interface utilisateur s'adapte à tous les types d'utilisateurs, des débutants en informatique aux personnes ayant de très bonnes connaissances techniques.

Le premier bouton indique le mode d'affichage actuel de l'interface utilisateur. Pour changer le mode de l'interface utilisateur, cliquez sur la flèche du bouton et sélectionnez le mode souhaité à partir du menu.

Mode	Description
Mode Débutant	Convient aux débutants en informatique et aux personnes qui souhaitent que BitDefender protège leur ordinateur et leurs données sans être interrompues. Ce mode est facile à utiliser et ne requiert de votre part que très peu d'interventions. Vous devez simplement corriger les problèmes rencontrés comme indiqué par BitDefender. Un assistant intuitif vous guidera pas à pas dans la résolution de ces problèmes. Vous pouvez également réaliser des tâches courantes comme la mise à jour des signatures de virus BitDefender et des fichiers du programme ou l'analyse de l'ordinateur.
Mode Intermédiaire	Conçu pour des utilisateurs ayant des compétences moyennes en informatique, ce mode étend les possibilités du Mode Débutant. Vous pouvez corriger les problèmes séparément et choisir les éléments à surveiller. De plus, vous pouvez gérer à distance les produits BitDefender installés sur les ordinateurs de votre foyer.
Mode Expert	Ce mode, qui convient à des utilisateurs ayant plus de connaissances techniques, vous permet de configurer

Mode	Description
	en détail chaque fonctionnalité de BitDefender. Vous pouvez également utiliser toutes les tâches fournies pour protéger votre ordinateur et vos données.

Réinitialisation du profil d'utilisation. . Le profil d'utilisation reflète les principales activités réalisées avec l'ordinateur. L'interface du produit s'adapte à votre profil d'utilisation pour vous permettre d'accéder facilement à vos tâches favorites.

Pour reconfigurer le profil d'utilisation, cliquez sur **Réinitialiser le Profil d'Utilisation** et suivez l'assistant de configuration.

8.2. Paramètres de sécurité

Vous pouvez activer ou désactiver des paramètres du produit couvrant plusieurs aspects de la sécurité informatique et des données dans cette zone. L'état actuel d'un paramètre est indiqué avec l'une des icônes suivantes :

Cercle vert coché : Le paramètre est activé.
Cercle rouge avec un point d'exclamation : Le paramètre est désactivé.

Pour activer/désactiver un paramètre, cochez/décochez la case **Activer** correspondante.

Avertissement

Soyez prudent(e) lorsque vous désactivez la protection antivirus en temps réel ou la mise à jour automatique. Désactiver ces fonctionnalités peut compromettre la sécurité de votre ordinateur. Si vous avez réellement besoin de les désactiver, pensez à les réactiver dès que possible.

Vous pouvez consulter la liste complète des paramètres et leur description dans le tableau suivant :

Paramètre	Description
Antivirus	La protection de fichiers en temps réel garantit que tous les fichiers sont analysés lorsque vous (ou une application exécutée sur ce système) y accédez.
Mise à jour automatique	La mise à jour automatique permet de télécharger et d'installer automatiquement et régulièrement les dernières versions du produit BitDefender et des fichiers de signatures.

Paramètre	Description
Contrôle de vulnérabilité	La vérification automatique des vulnérabilités s'assure que les logiciels majeurs de votre ordinateur sont à jour.
Antiphishing	L'Antiphishing vous alerte en temps réel s'il détecte qu'une page Web est conçue pour voler des informations personnelles.
Contrôle d'Identité	Le Contrôle d'Identité vous aide à empêcher que vos données personnelles ne soient transmises sur Internet sans votre accord. Il bloque tous les messages instantanés, e-mails ou formulaires Web transmettant vers des destinataires non autorisés des données que vous avez définies comme étant confidentielles.
Cryptage de messagerie instantanée	Le cryptage de Messagerie Instantanée protège vos conversations via Yahoo! Messenger et Windows Live Messenger à condition que vos contacts de messagerie instantanée utilisent un produit BitDefender et un logiciel de messagerie instantanée compatibles.

L'état de certains de ces paramètres peut être surveillé par le système de contrôle de BitDefender. Si vous désactivez un paramètre surveillé, BitDefender le signalera comme un problème à corriger.

Si vous ne souhaitez pas qu'un paramètre surveillé que vous avez désactivé soit signalé comme un problème, vous devez configurer le système de contrôle de façon adaptée. Vous pouvez le faire en Mode Intermédiaire ou en Mode Expert.

- En Mode Intermédiaire, le système de contrôle peut être configuré à partir de différents endroits, en fonction des catégories de paramètres. Pour plus d'informations, veuillez vous référer à la partie « Mode Intermédiaire » (p. 74) de ce guide d'utilisation.
- En Mode Expert, le système de contrôle peut être configuré à partir d'un emplacement central. Suivez ces étapes :
  1. Allez dans **Général>Tableau de bord**.
  2. Cliquez sur **Configurer le système de contrôle d'état**.
  3. Décochez la case correspondant à l'élément que vous ne souhaitez pas surveiller.

  Pour plus d'informations, reportez-vous au chapitre « *État* » (p. 97).

8.3. Paramètres généraux

Dans cette zone, vous pouvez activer ou désactiver les paramètres qui affectent le fonctionnement du produit et son utilisation. Pour activer/désactiver un paramètre, cochez/décochez la case **Activer** correspondante.

Vous pouvez consulter la liste complète des paramètres et leur description dans le tableau suivant :

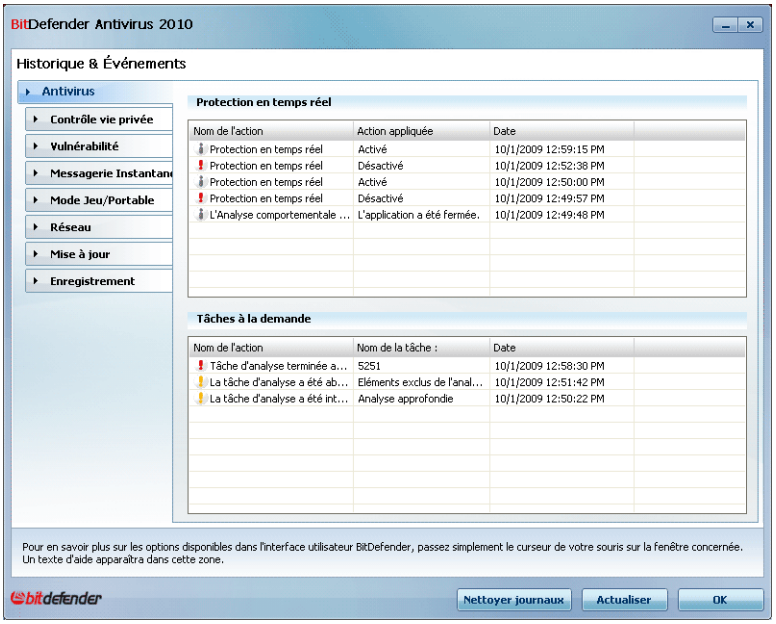
Paramètre	Description
Mode jeu	Le mode Jeu modifie de manière temporaire les paramètres de protection afin de préserver les ressources de votre système pendant les jeux.
Détection du Mode Portable	Le Mode Portable modifie de manière temporaire les paramètres de protection afin de préserver l'autonomie de la batterie de votre ordinateur portable.
Mot de passe pour les paramètres	Cette option garantit que les paramètres BitDefender ne puissent être modifiés que par une personne connaissant ce mot de passe. Si vous activez cette option, on vous demandera de configurer le mot de passe des paramètres. Tapez le mot de passe souhaité dans les deux champs et cliquez sur **OK** pour définir le mot de passe.
BitDefender News	En activant cette option, vous serez informé par BitDefender de l'actualité de la société, des mises à jour de produits ou des nouvelles menaces de sécurité.
Alertes de notification du produit	En activant cette option, vous recevrez des alertes d'information.
Barre d'activité d'analyse	La Barre d'Activité d'Analyse est une petite fenêtre transparente indiquant la progression de l'activité d'analyse de BitDefender. Pour plus d'informations, reportez-vous à « *Barre de l'activité d'analyse* » (p. 32).
Envoyer rapports d'infection	En activant cette option, les rapports d'analyse virale sont envoyés aux laboratoires BitDefender pour être examinés. Notez que ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et qu'ils ne seront pas utilisés à des fins commerciales.
Détection des alertes	En activant cette option, les rapports concernant les potentielles alertes virales sont envoyés aux

Paramètre	Description
	laboratoires BitDefender pour être examinés. Notez que ces rapports ne comprendront aucune donnée confidentielle, telle que votre nom ou votre adresse IP, et qu'ils ne seront pas utilisés à des fins commerciales.

9. Historique et Événements

Le lien **Afficher les Journaux** situé en bas de la fenêtre principale de BitDefender ouvre une autre fenêtre contenant l'historique et les événements de BitDefender. Cette fenêtre vous présente les événements liés à la sécurité. Par exemple, vous pouvez facilement vérifier qu'une mise à jour s'est effectuée correctement, s'il y a eu des malwares détectés sur votre ordinateur, etc.

Note
Le lien est seulement accessible en Mode Intermédiaire ou en Mode Expert.



Événements

Les catégories suivantes, présentées à gauche, permettent de filtrer l'historique et les événements BitDefender:

- **Antivirus**
- **Contrôle Vie privée**
- **Vulnérabilité**
- **Cryptage de messagerie instantanée**
- **Mode Jeu/Portable**

- **Réseau Domestique**
- **Mise-à-jour**
- **Enregistrement**
- **Journal Internet**

Une liste d'événements est proposée pour chaque catégorie. Chaque événement comporte les informations suivantes : une courte description de l'événement, l'action menée par BitDefender, la date et l'heure de l'événement. Pour obtenir plus d'informations sur un événement de la liste en particulier, double-cliquez sur cet événement.

Cliquez sur **Effacer tous les journaux** si vous voulez supprimer les anciens journaux ou sur **Actualiser** pour vous assurer que les journaux les plus récents sont affichés.

10. Enregistrement et Mon compte

BitDefender Antivirus 2010 a une période d'essai de 30 jours. Pendant la période d'essai, toutes les fonctionnalités du programme sont disponibles et vous pouvez donc tester le produit pour voir s'il répond à vos attentes. Veuillez noter qu'après 15 jours d'essai, le produit ne se mettra plus à jour, à moins que vous ne créiez un compte BitDefender. La création d'un compte BitDefender est une étape obligatoire du processus d'enregistrement.

Avant que la période d'essai ne soit passée, vous devez enregistrer le produit afin que votre ordinateur continue à être protégé. L'enregistrement se fait en deux étapes :

1. **Activation du produit (enregistrement d'un compte BitDefender).** Vous devez créer un compte BitDefender afin de recevoir les mises à jour et d'avoir accès au support technique gratuit. Si vous avez déjà un compte BitDefender, enregistrez votre produit BitDefender avec ce compte. Si vous avez besoin d'activer votre produit, BitDefender vous le signalera et vous aidera à régler ce problème.

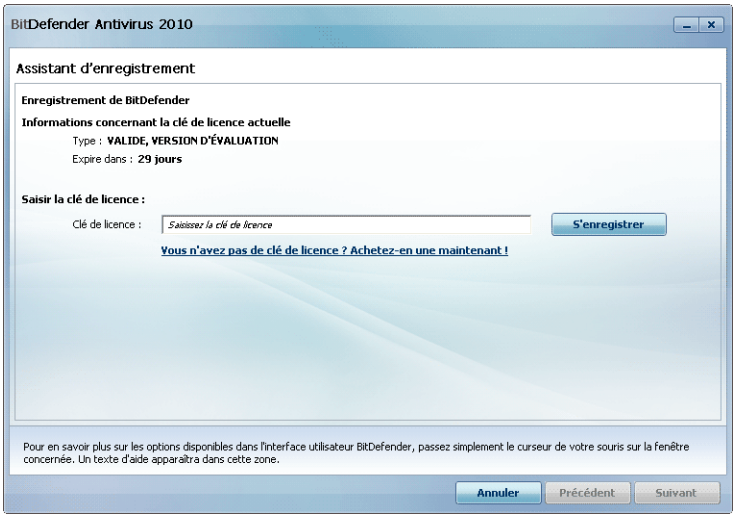
   Important

   Vous devez créer un compte dans les 15 jours après l'installation de BitDefender (si vous l'enregistrez avec une clé de licence, l'expiration est repoussée à 30 jours). Dans le cas contraire, BitDefender ne se mettra plus à jour.

2. **Enregistrement avec une clé de licence.** La clé de licence indique pendant combien de temps vous pouvez utiliser le produit. Dès que la clé de licence expire, BitDefender cesse de réaliser ses fonctions et de protéger votre ordinateur. Vous devez enregistrer le produit avec une clé de licence lorsque la période d'essai se termine. Nous vous recommandons d'acheter une clé de licence ou de renouveler votre licence quelques jours avant l'expiration de la clé utilisée.

10.1. Enregistrement de BitDefender Antivirus 2010

Si vous souhaitez enregistrer le produit avec une clé de licence ou changer la clé de licence actuelle, cliquez sur le lien **S'enregistrer** situé en bas de la fenêtre BitDefender. La fenêtre d'enregistrement du produit s'affichera.


BitDefender Antivirus 2010
Assistant d'enregistrement
Enregistrement de BitDefender
Informations concernant la clé de licence actuelle
Type : VALIDE, VERSION D'ÉVALUATION
Expire dans : 29 jours
Saisir la clé de licence :
Clé de licence :
Saisissez la clé de licence
S'enregistrer
Vous n'avez pas de clé de licence ? Achetez-en une maintenant !
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Suivant

Enregistrement

Vous pouvez visualiser l'état de votre enregistrement BitDefender, votre clé d'activation actuelle ou voir dans combien de jours la licence arrivera à son terme.

Pour enregistrer BitDefender Antivirus 2010 :

1. Entrez la clé d'activation dans le champ de saisie.

   Note
   Vous trouverez votre clé d'activation :
   - sur l'étiquette du CD.
   - sur la carte d'enregistrement du produit.
   - sur l'e-mail d'achat en ligne.

   Si vous n'avez pas de clé d'activation BitDefender, cliquez sur le lien indiqué pour être dirigé vers la boutique en ligne BitDefender et en acheter une.

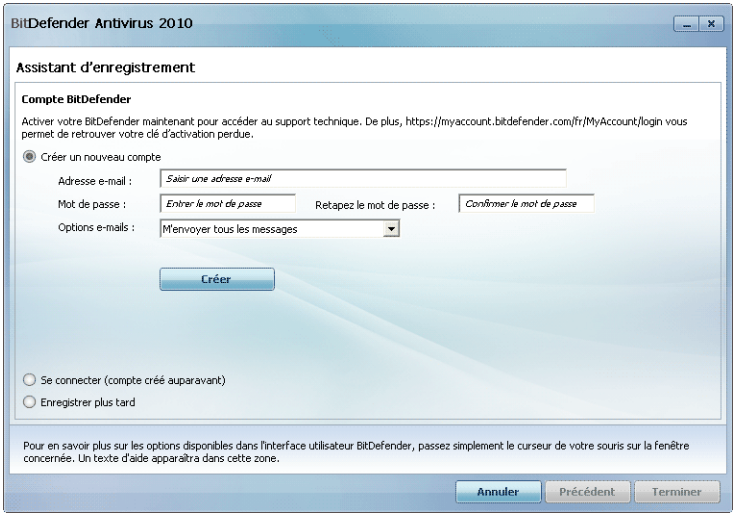
2. Cliquez sur **S'enregistrer**.
3. Cliquez sur **Terminer**.

10.2. Activation de BitDefender

Pour activer BitDefender, vous devez créer un compte BitDefender ou vous connecter à un compte existant. Si vous n'avez pas enregistré de compte BitDefender pendant l'assistant d'enregistrement initial, procédez comme suit :

- En Mode Débutant, cliquez sur **Corriger tous les problèmes**. L'assistant vous aidera à corriger les problèmes en attente, y compris l'activation du produit.
- En Mode Intermédiaire, allez dans l'onglet **Sécurité** et cliquez sur le bouton **Corriger** correspondant au problème de l'activation du produit.
- En Mode Expert, allez dans **Enregistrement** et cliquez sur le bouton **Activer le produit**.

Une fenêtre d'enregistrement du compte s'ouvrira. C'est là que vous pouvez créer un compte BitDefender ou vous connecter à un compte existant pour activer votre produit.


BitDefender Antivirus 2010
Assistant d'enregistrement
Compte BitDefender
Activer votre BitDefender maintenant pour accéder au support technique. De plus, https://myaccount.bitdefender.com/fr/MyAccount/login vous permet de retrouver votre clé d'activation perdue.
Créer un nouveau compte
Adresse e-mail :
Saisir une adresse e-mail
Mot de passe :
Entrer le mot de passe
Retapez le mot de passe :
Confirmer le mot de passe
Options e-mails :
M'envoyer tous les messages
Créer
Se connecter (compte créé auparavant)
Enregistrer plus tard
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Terminer

Création de compte

Si vous ne souhaitez pas créer immédiatement un compte BitDefender, sélectionnez **Enregistrer plus tard** et cliquez sur **Terminer**. Autrement, procédez selon votre situation actuelle :

- « Je n'ai pas de compte BitDefender » (p. 53)
- « J'ai déjà un compte BitDefender » (p. 53)

Important

Vous devez créer un compte dans les 15 jours après l'installation de BitDefender (si vous l'enregistrez avec une clé de licence, l'expiration est repoussée à 30 jours). Dans le cas contraire, BitDefender ne se mettra plus à jour.

Je n'ai pas de compte BitDefender

Pour créer un compte BitDefender, suivez ces étapes :

1. Sélectionnez **Créer un nouveau compte**.
2. Tapez les informations requises dans les champs correspondants. Les informations communiquées ici resteront confidentielles.
   - **E-mail** - entrez votre adresse e-mail.
   - **Mot de passe** - entrez un mot de passe pour votre compte BitDefender. Le mot de passe doit contenir entre 6 et 16 caractères.
   - **Retaper le mot de passe** - re-entrez le mot de passe choisi auparavant.

   Note
   Une fois le compte activé, vous pouvez utiliser l'adresse e-mail et le mot de passe indiqués pour vous connecter à votre compte sur http://myaccount.bitdefender.com.

3. Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte. Sélectionnez l'une des options disponibles dans le menu :
   - **M'envoyer tous les messages**
   - **M'envoyer seulement les messages concernant le produit**
   - **Je ne veux recevoir aucun message**
4. Cliquez sur **Créer**.
5. Cliquez sur **Terminer** pour quitter l'assistant.
6. **Activez votre compte.** Vous devez activez votre compte avant de pouvoir l'utiliser. Consultez votre messagerie et suivez les instructions données dans le message que vous a adressé le service d'enregistrement de BitDefender.

J'ai déjà un compte BitDefender

BitDefender détectera automatiquement si vous avez déjà un compte BitDefender actif sur cet ordinateur. Dans ce cas, indiquez le mot de passe de votre compte et cliquez sur **Se connecter**. Cliquez sur **Terminer** pour quitter l'assistant.

Si vous avez déjà un compte actif, mais que BitDefender ne le détecte pas, suivez ces étapes pour enregistrer le produit avec ce compte :

1. Sélectionnez **Se connecter (compte créé auparavant)**.
2. Tapez l'adresse e-mail et le mot de passe de votre compte dans les champs correspondants.

Note
Si vous ne souhaitez pas faire de modifications, cliquez sur **Terminer** pour fermer l'assistant.

3. Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte. Sélectionnez l'une des options disponibles dans le menu :
   - **M'envoyer tous les messages**
   - **M'envoyer seulement les messages concernant le produit**
   - **Je ne veux recevoir aucun message**
4. Cliquez sur **Se connecter**.
5. Cliquez sur **Terminer** pour quitter l'assistant.

10.3. Achat de clés de licence

Si la période d'essai est sur le point d'expirer, vous devez acheter une clé de licence et enregistrer votre produit. Ouvrez BitDefender et cliquez sur le lien **Acheter/Renouveler** situé en bas de la fenêtre. Le lien vous conduit vers une page Web où vous pouvez acheter une clé de licence pour votre produit BitDefender.

10.4. Renouvellement de votre licence

En tant que client BitDefender, vous avez droit à une réduction lorsque vous renouvelez la licence de votre produit BitDefender. Vous pouvez également mettre à niveau votre produit vers la version actuelle à un tarif spécial ou gratuitement.

Si votre clé de licence actuelle est sur le point d'expirer, vous devez renouveler votre licence. Ouvrez BitDefender et cliquez sur le lien **Acheter/Renouveler** situé en bas de la fenêtre. Le lien vous conduit vers une page Web où vous pouvez renouveler votre licence.

11. Assistants

Afin que BitDefender soit très simple à utiliser, plusieurs assistants vous aident à réaliser des tâches de sécurité spécifiques et à configurer des paramètres du produit plus complexes. Ce chapitre décrit les assistants pouvant apparaître lorsque vous corrigez des problèmes ou effectuez des tâches spécifiques avec BitDefender. D'autres assistants de configuration son décrits séparément dans la partie « Mode Expert » (p. 96).

11.1. Assistant d'analyse antivirus

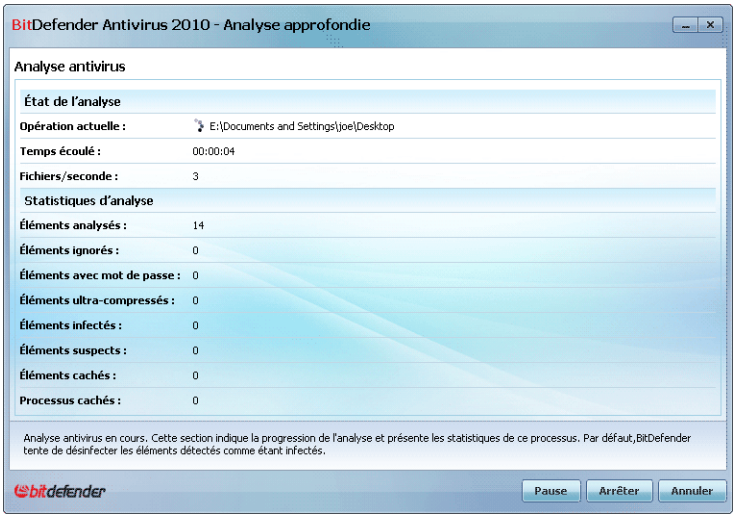
À chaque fois que vous initierez une analyse à la demande (par exemple en faisant un clic droit sur un dossier et en sélectionnant **Analyser avec BitDefender**), l'assistant de l'analyse antivirus s'affichera. Suivez cette procédure en trois étapes pour effectuer le processus d'analyse:

Note

Si l'assistant d'analyse ne s'affiche pas, il est possible que l'analyse soit paramétrée pour s'exécuter invisiblement, en tâche de fond. Recherchez l'icône de l'avancement de l'analyse dans la barre des tâches. Vous pouvez cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

11.1.1. Étape 1 sur 3 - Analyse

BitDefender commence à analyser les objets sélectionnés.


BitDefender Antivirus 2010 - Analyse approfondie
Analyse antivirus
État de l'analyse
Opération actuelle : E:\Documents and Settings\joe\Desktop
Temps écoulé : 00:00:04
Fichiers/seconde : 3
Statistiques d'analyse
Éléments analysés : 14
Éléments ignorés : 0
Éléments avec mot de passe : 0
Éléments ultra-compressés : 0
Éléments infectés : 0
Éléments suspects : 0
Éléments cachés : 0
Processus cachés : 0
Analyse antivirus en cours. Cette section indique la progression de l'analyse et présente les statistiques de ce processus. Par défaut,BitDefender tente de désinfecter les éléments détectés comme étant infectés.
bitdefender
Pause
Arrêter
Annuler

Analyse en cours

Le statut et les statistiques de l'analyse s'affichent (vitesse d'analyse, temps écoulé, nombre d'objets analysés / infectés / suspects / cachés, etc.).

Patientez jusqu'à ce que BitDefender ait terminé l'analyse.

Note
L'analyse peut durer un certain temps, suivant sa complexité.

Archives protégées par mot de passe. Si BitDefender détecte pendant l'analyse une archive protégée par mot de passe, et que l'action par défaut est **Demander le mot de passe**, vous serez invité à fournir le mot de passe. Les archives protégées par mot de passe ne peuvent pas être analysées à moins que vous ne communiquiez le mot de passe. Voici les options proposées :

- **Je souhaite saisir le mot de passe de cet objet.** Si vous souhaitez que BitDefender analyse l'archive, sélectionnez cette option et entrez le mot de passe. Si vous ne connaissez pas le mot de passe, choisissez l'une des autres options.
- **Je ne souhaite pas saisir le mot de passe de cet objet (ignorer cet objet).** Sélectionnez cette option pour ne pas analyser cette archive.
- **Je ne souhaite saisir le mot de passe d'aucun objet (ignorer tous les objets protégés par un mot de passe).** Sélectionnez cette option si vous ne voulez pas être dérangé au sujet des archives protégées par mot de passe.

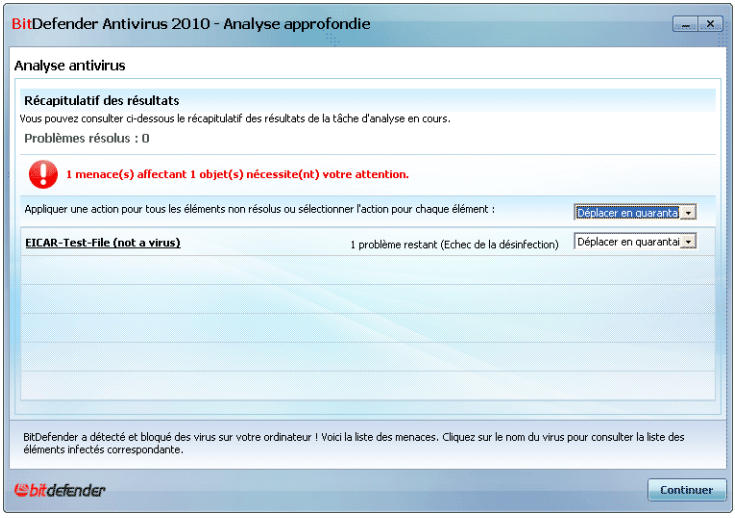
BitDefender ne pourra pas les analyser, mais un rapport sera conservé dans le journal des analyses.

Cliquez sur **OK** pour continuer l'analyse.

Arrêt ou pause de l'analyse. Vous pouvez arrêter l'analyse à tout moment en cliquant sur **Arrêter et Oui**. Vous vous retrouverez alors à la dernière étape de l'assistant. Pour suspendre temporairement le processus d'analyse, cliquez sur **Pause**. Pour reprendre l'analyse, cliquez sur **Reprendre**.

11.1.2. Étape 2 sur 3 - Sélectionner des actions

Une fois l'analyse terminée, une nouvelle fenêtre apparaît affichant les résultats de l'analyse.


BitDefender Antivirus 2010 - Analyse approfondie
Analyse antivirus
Récapitulatif des résultats
Vous pouvez consulter ci-dessous le récapitulatif des résultats de la tâche d'analyse en cours.
Problèmes résolus : 0
1 menace(s) affectant 1 objet(s) nécessite(nt) votre attention.
Appliquer une action pour tous les éléments non résolus ou sélectionner l'action pour chaque élément :
Déplacer en quaranta
EICAR-Test-File (not a virus)
1 problème restant (Echec de la désinfection)
Déplacer en quarantai
BitDefender a détecté et bloqué des virus sur votre ordinateur ! Voici la liste des menaces. Cliquez sur le nom du virus pour consulter la liste des éléments infectés correspondante.
bitdefender
Continuer

Actions

Le nombre de problèmes de sécurité affectant votre système est indiqué.

Les objets infectés sont affichés dans des groupes, basés sur les malwares les ayant infectés. Cliquez sur le lien correspondant à une menace pour obtenir plus d'informations sur les éléments infectés.

Vous pouvez sélectionner une action globale à mener pour l'ensemble des problèmes de sécurité ou sélectionner des actions spécifiques pour chaque groupe de problèmes.

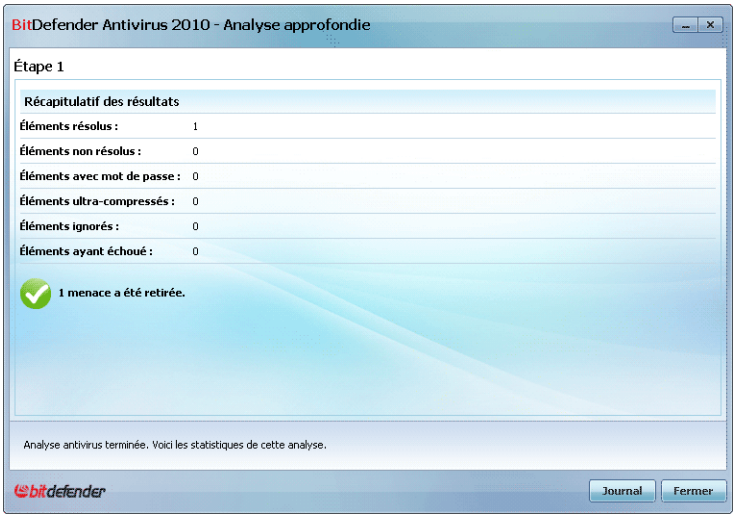
Une ou plusieurs des options qui suivent peuvent apparaître dans le menu :

Action	Description
Ne pas mener d'action	Aucune action ne sera menée sur les fichiers détectés. Une fois l'analyse terminée, vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.
Désinfecter	Supprime le code malveillant des fichiers infectés.
Supprimer	Supprime les fichiers détectés.
Quarantaine	Déplace les fichiers detectés dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.
Renommer	Modifie le nom des fichiers cachés en y ajoutant le suffixe `.bd.ren`. Vous pourrez ainsi rechercher ce type de fichiers sur votre ordinateur, et les trouver s'il en existe. Veuillez noter que ces fichiers cachés ne sont pas ceux que vous avez choisi de ne pas afficher dans Windows. Ce sont des fichiers qui ont été cachés par des programmes particuliers, connus sous le nom de rootkits. Les rootkits ne sont pas malveillants en eux-mêmes. Ils sont cependant couramment utilisés pour rendre les virus et les spywares indétectables par les programmes antivirus habituels.

Cliquez sur **Continuer** pour appliquer les actions spécifiées.

11.1.3. Étape 3 sur 3 - Voir les résultats

Une fois que les problèmes de sécurité auront été corrigés par BitDefender, les résultats de l'analyse apparaîtront dans une nouvelle fenêtre.


BitDefender Antivirus 2010 - Analyse approfondie
Étape 1
Récapitulatif des résultats
Éléments résolus : 1
Éléments non résolus : 0
Éléments avec mot de passe : 0
Éléments ultra-compressés : 0
Éléments ignorés : 0
Éléments ayant échoué : 0
1 menace a été retirée.
Analyse antivirus terminée. Voici les statistiques de cette analyse.
bitdefender
Journal
Fermer

Récapitulatif

Le récapitulatif des résultats s'affiche. Si vous souhaitez connaître toutes les informations sur le processus d'analyse, cliquez sur **Afficher le fichier journal** pour afficher le journal des analyses.

Important
Si cela est nécessaire, il vous sera demandé de redémarrer votre système pour terminer le processus d'installation.

Cliquez sur **Fermer** pour fermer la fenêtre.

BitDefender n'a pas pu corriger certains problèmes

Dans la plupart des cas, BitDefender désinfecte ou isole l'infection des fichiers infectés qu'il détecte. Cependant, il y a des problèmes qui ne peuvent pas être résolus.

Dans ces cas, nous vous recommandons de contacter le support BitDefender sur le site www.bitdefender.fr. Nos équipes du support technique vous aideront à résoudre les problèmes que vous rencontrez.

BitDefender a détecté des fichiers suspects

Les fichiers suspects sont des fichiers détectés par l'analyse heuristique pouvant être infectés par des malwares et pour lesquels une signature n'a pas encore été publiée.

Lorsque des fichiers suspects seront détectés durant l'analyse, vous serez invité à les envoyer au laboratoire BitDefender. Cliquez sur **OK** pour envoyer ces fichiers aux laboratoires BitDefender pour une analyse plus approfondie.

11.2. Assistant d'Analyse Personnalisée

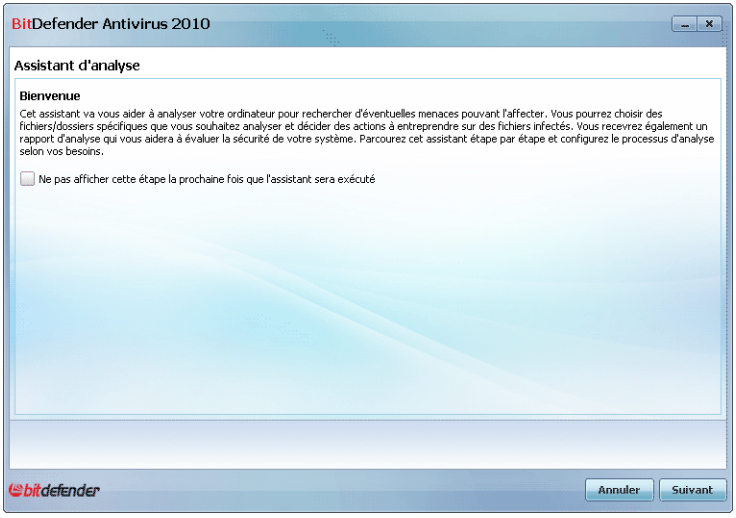
L'Assistant d'Analyse Personnalisée vous permet de créer et de lancer une tâche d'analyse personnalisée et éventuellement de l'enregistrer comme Tâche Rapide si vous utilisez BitDefender en Mode Intermédiaire.

Pour lancer une tâche d'analyse personnalisée à l'aide de l'Assistant d'Analyse Personnalisée, suivez ces étapes :

1. En Mode Intermédiaire, cliquez sur l'onglet **Antivirus**.
2. Dans la zone Tâches rapides, cliquez sur **Analyse personnalisée**.
3. Suivez cette procédure en six étapes pour effectuer le processus d'analyse.

11.2.1. Etape 1 sur 6 – Fenêtre de Bienvenue

Il s'agit d'une fenêtre d'accueil.


BitDefender Antivirus 2010
Assistant d'analyse
Bienvenue
Cet assistant va vous aider à analyser votre ordinateur pour rechercher d'éventuelles menaces pouvant l'affecter. Vous pourrez choisir des fichiers/dossiers spécifiques que vous souhaitez analyser et décider des actions à entreprendre sur des fichiers infectés. Vous recevrez également un rapport d'analyse qui vous aidera à évaluer la sécurité de votre système. Parcourez cet assistant étape par étape et configurez le processus d'analyse selon vos besoins.
Ne pas afficher cette étape la prochaine fois que l'assistant sera exécuté
bitdefender
Annuler
Suivant

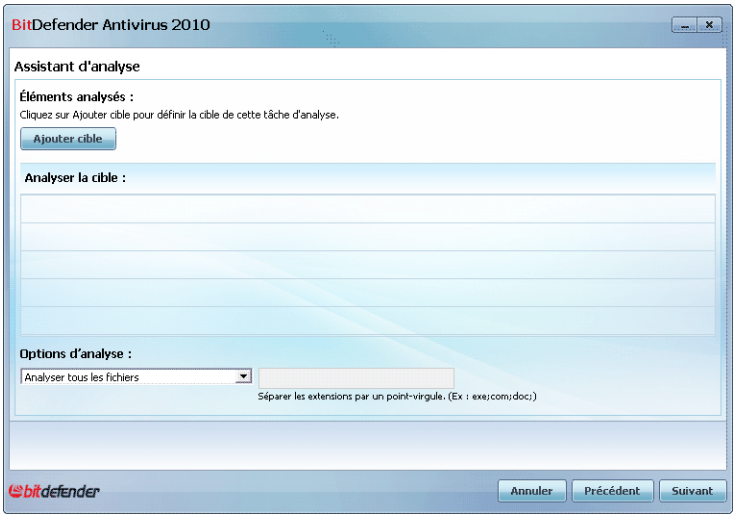
Page d'accueil

Si vous voulez ignorer cette fenêtre la prochaine fois que vous lancerez cet assistant, cochez la case **Ne pas afficher cette étape lors de la prochaine exécution de l'assistant**.

Cliquez sur **Suivant**.

11.2.2. Étape 2/6 - Sélectionner la Cible

Vous pouvez spécifier dans cette rubrique les fichiers et les dossiers à analyser ainsi que les options d'analyse.



Sélectionner la Cible

Cliquez sur **Ajouter une cible**, sélectionnez les fichiers ou les dossiers que vous souhaitez analyser et cliquez sur **OK**. Les chemins vers les emplacements sélectionnés apparaîtront dans la colonne **Cible de l'Analyse**. Si vous changez d'avis pour un emplacement donné, cliquez simplement sur le bouton **Supprimer** situé en regard de l'emplacement. Cliquez sur le bouton **Tout Supprimer** pour supprimer tous les emplacements ajoutés à la liste.

Une fois les emplacements sélectionnés, définissez les **Options d'Analyse**. Les options suivantes sont disponibles :

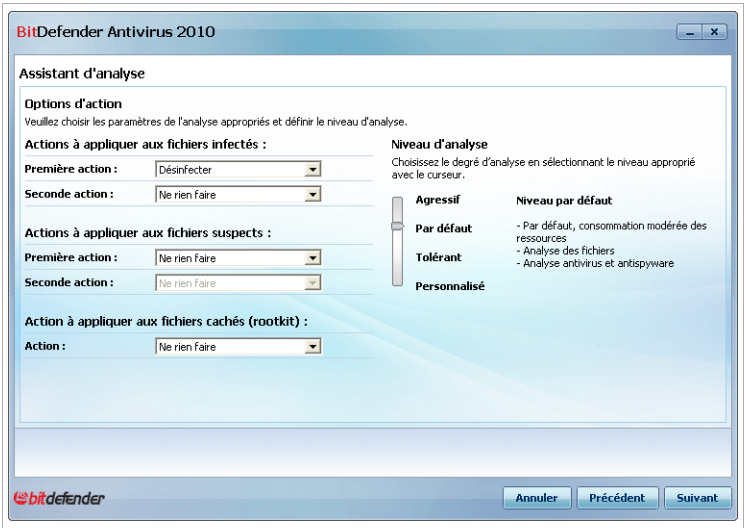
Option	Description
Analyse de tous les fichiers	Sélectionnez cette option pour analyser tous les fichiers des dossiers sélectionnés.
Analyser uniquement les fichiers ayant des	Seuls les fichiers avec les extensions suivantes seront analysés : `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`;

Option	Description
extensions d'applications	.ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml et .nws.
Analyser uniquement les extensions définies par l'utilisateur	Seuls les fichiers avec les extensions définies par l'utilisateur seront analysés. Ces extensions doivent être séparées par ";".

Cliquez sur **Suivant**.

11.2.3. Étape 3/6 - Sélectionner les Actions

Vous pouvez définir dans cette rubrique les paramètres et le niveau d'analyse.



Sélectionner les Actions

- Sélectionnez les actions à appliquer contre les fichiers infectés et suspects détectés. Voici les options proposées :

Action	Description
Ne pas mener d'action	Aucune action ne sera prise sur les fichiers infectés. Ceux-ci vont apparaître dans le fichier des rapports.
Désinfecter	Supprimer le code malveillant des fichiers infectés.
Supprimer les fichiers	Supprime immédiatement les fichiers infectés, sans avertissement.
Déplacer vers la quarantaine	Déplace les fichiers infectés dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.

- Sélectionnez l'action à appliquer aux fichiers cachés (rootkits). Voici les options proposées :

Action	Description
Ne pas mener d'action	Aucune mesure ne sera prise à l'encontre des fichiers cachés. Ces fichiers apparaîtront dans le fichier rapport.
Renommer	Modifie le nom des fichiers cachés en y ajoutant le suffixe `.bd.ren`. Vous pourrez ainsi rechercher ce type de fichiers sur votre ordinateur, et les trouver s'il en existe.

- Configurer le degré d'analyse. Vous pouvez choisir parmi 3 niveaux de protection. Sélectionnez le niveau approprié avec le curseur :

Niveau d'analyse	Description
Tolérant	Seuls les fichiers d'applications font l'objet d'une analyse antivirus. La consommation de ressources est faible.
Par défaut	La consommation de ressources est modérée. Tous les fichiers font l'objet d'une analyse antivirus et antispyware.
Agressif	Tous les fichiers (y compris les archives) font l'objet d'une analyse antivirus et antispyware. Les processus et les fichiers cachés sont inclus dans l'analyse. La consommation de ressources est plus élevée.

Les utilisateurs avancés peuvent vouloir profiter des paramètres d'analyse de BitDefender. L'analyse peut être configurée pour rechercher uniquement un

certain type de malwares. Cela peut réduire considérablement la durée de l'analyse et améliorer la réactivité de votre ordinateur pendant les analyses.

Déplacez le curseur pour sélectionner **Personnalisé** puis cliquez sur le bouton **Niveau personnalisé**. Une fenêtre s'affichera. Spécifiez le type de malwares que vous souhaitez que BitDefender recherche en sélectionnant les options appropriées :

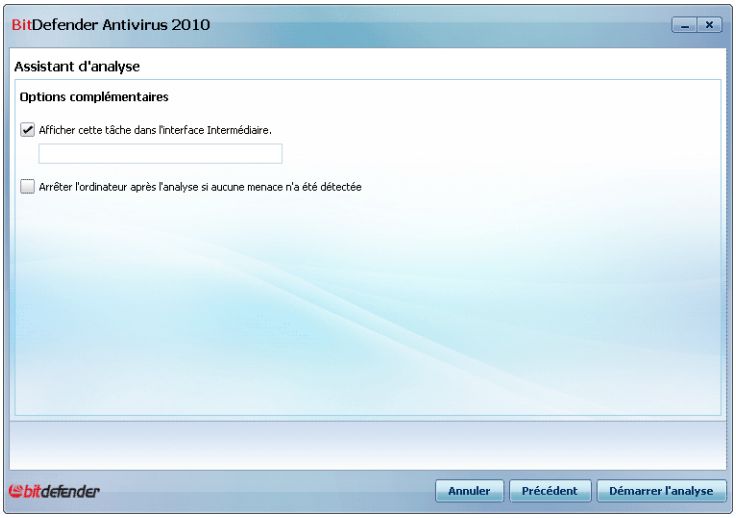
Option	Description
Analyse antivirus	Analyse les virus connus. BitDefender détecte également les corps de virus incomplets, permettant ainsi d'écarter toute menace potentielle pouvant affecter la sécurité de votre système.
Détecter les adwares	Analyse les menaces d'adwares. Les fichiers détectés sont traités en tant que fichiers infectés. Un logiciel incluant des composants de type adware peut ne plus fonctionner si cette option est activée.
Rechercher les spywares	Analyse les menaces de spywares connus. Les fichiers détectés sont traités en tant que fichiers infectés.
Analyser les applications	Analyser les applications légitimes qui pourraient être utilisées pour cacher des outils d'espionnage ou d'autres applications malicieuses.
Détecter les numéroteurs	Analyse les applications qui appellent des numéros surtaxés. Les fichiers détectés sont traités en tant que fichiers infectés. Un logiciel incluant des composants de type numéroteur peut ne plus fonctionner si cette option est activée.
Analyse des rootkits	Analyse les objets cachés (fichiers et processus), plus connus sous le nom de rootkits.
Rechercher les keyloggers	Recherche la présence d'applications malveillantes enregistrant les frappes au clavier.

Cliquez sur **OK** pour fermer la fenêtre.

Cliquez sur **Suivant**.

11.2.4. Étape 4/6 - Paramètres Supplémentaires

Avant que l'analyse ne commence, des options supplémentaires sont disponibles :



Paramètres Supplémentaires

- Pour enregistrer la tâche personnalisée que vous créez afin de la réutiliser, cochez la case **Afficher cette tâche dans l'interface utilisateur Intermédiaire** et entrez le nom de cette tâche dans le champ de saisie.

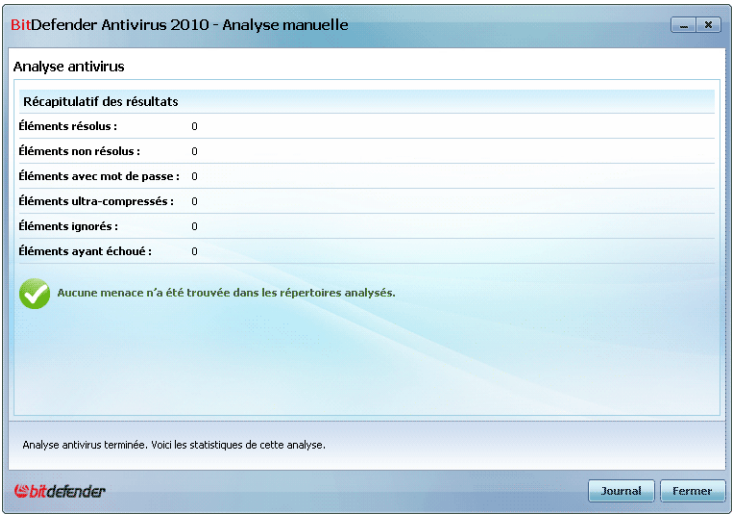
  La tâche sera ajoutée à la liste des Tâches Rapides déjà disponibles dans l'onglet Sécurité et apparaîtra aussi dans **Mode Expert > Antivirus > Analyse Antivirus**.

- Pour éteindre l'ordinateur à la fin de l'analyse cochez la case **Éteindre l'ordinateur à la fin de l'analyse si aucune menace n'est trouvée**.

Cliquez sur **Démarrer l'analyse**.

11.2.5. Étape 5/6 - Analyse

BitDefender commencera à analyser les objets sélectionnés :


BitDefender Antivirus 2010 - Analyse manuelle
Analyse antivirus
Récapitulatif des résultats
Éléments résolus : 0
Éléments non résolus : 0
Éléments avec mot de passe : 0
Éléments ultra-compressés : 0
Éléments ignorés : 0
Éléments ayant échoué : 0
Aucune menace n'a été trouvée dans les répertoires analysés.
Analyse antivirus terminée. Voici les statistiques de cette analyse.
bitdefender
Journal
Fermer

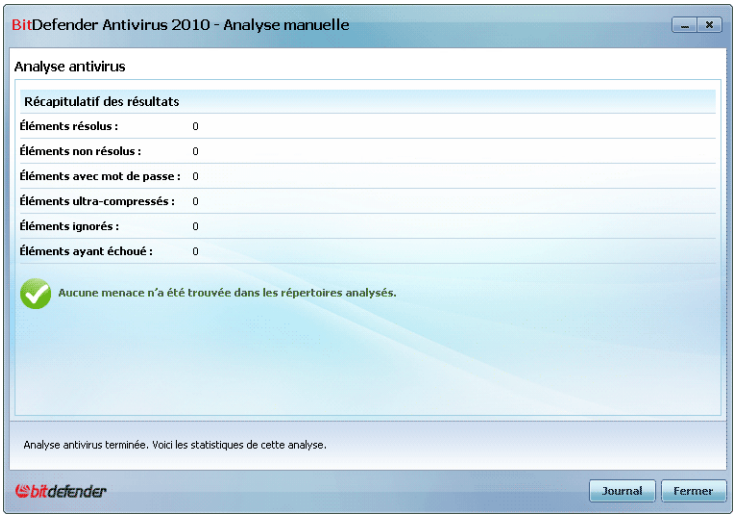
Analyse en cours

Note

L'analyse peut durer un certain temps, suivant sa complexité. Vous pouvez cliquer sur l'icône d'avancement de l'analyse dans la zone de notification pour ouvrir la fenêtre de l'analyse et voir l'avancement de l'analyse.

11.2.6. Étape 6/6 - Voir les résultats

Lorsque BitDefender aura terminé le processus d'analyse, les résultats de l'analyse apparaîtront dans une nouvelle fenêtre :


BitDefender Antivirus 2010 - Analyse manuelle
Analyse antivirus
Récapitulatif des résultats
Éléments résolus : 0
Éléments non résolus : 0
Éléments avec mot de passe : 0
Éléments ultra-compressés : 0
Éléments ignorés : 0
Éléments ayant échoué : 0
Aucune menace n'a été trouvée dans les répertoires analysés.
Analyse antivirus terminée. Voici les statistiques de cette analyse.
bitdefender
Journal
Fermer

Récapitulatif

Vous pouvez voir le résumé des résultats. Si vous souhaitez connaître toutes les informations sur le processus d'analyse, cliquez sur **Afficher le journal** pour afficher le journal de l'analyse.

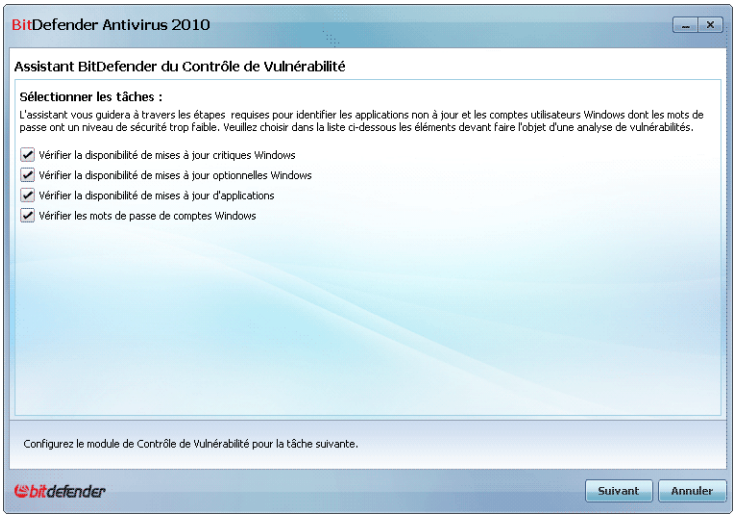
Important
Si cela est nécessaire, il vous sera demandé de redémarrer votre système pour terminer le processus d'installation.

Cliquez sur **Fermer** pour fermer la fenêtre.

11.3. Assistant du Contrôle de Vulnérabilité

L'assistant recherche la présence de vulnérabilités sur votre système et vous aide à les corriger.

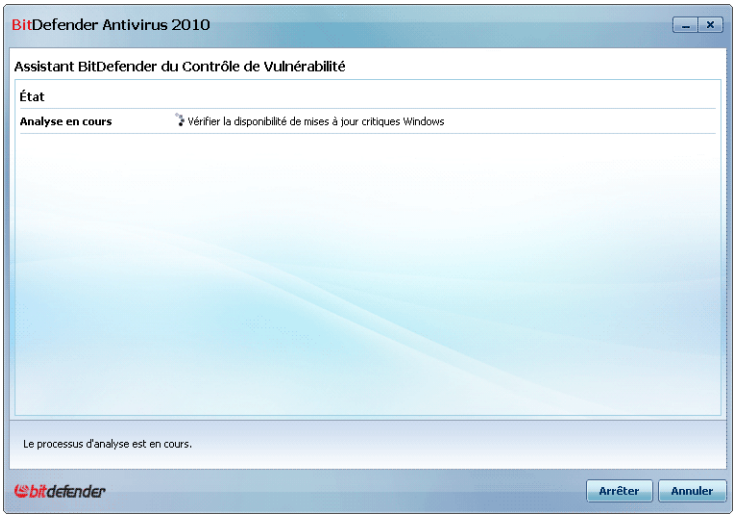
11.3.1. Etape 1/6 - Sélectionnez les vulnérabilités à vérifier


BitDefender Antivirus 2010
Assistant BitDefender du Contrôle de Vulnérabilité
Sélectionner les tâches :
L'assistant vous guidera à travers les étapes requises pour identifier les applications non à jour et les comptes utilisateurs Windows dont les mots de passe ont un niveau de sécurité trop faible. Veuillez choisir dans la liste ci-dessous les éléments devant faire l'objet d'une analyse de vulnérabilités.
Vérifier la disponibilité de mises à jour critiques Windows
Vérifier la disponibilité de mises à jour optionnelles Windows
Vérifier la disponibilité de mises à jour d'applications
Vérifier les mots de passe de comptes Windows
Configurez le module de Contrôle de Vulnérabilité pour la tâche suivante.
bitdefender
Suivant
Annuler

Vulnérabilités

Cliquez sur **Suivant** pour lancer l'analyse des vulnérabilités sélectionnées.

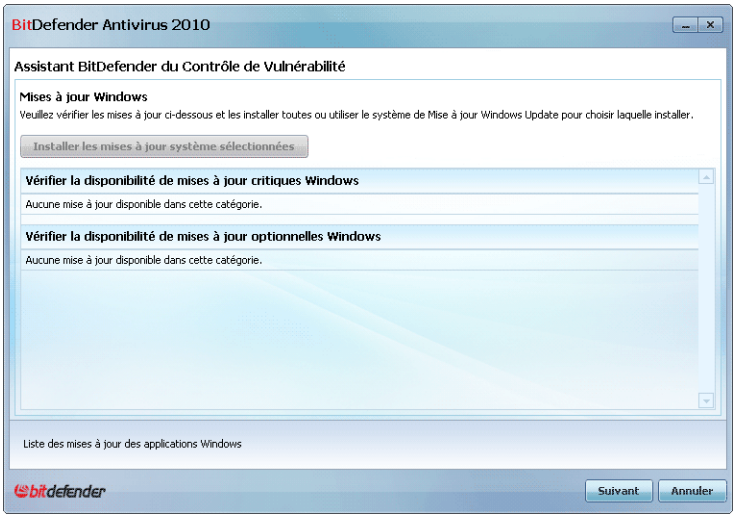
11.3.2. Etape 2/6 - Vérifier les vulnérabilités



Contrôle de vulnérabilité

Patientez jusqu'à ce que BitDefender ait terminé l'analyse des vulnérabilités.

11.3.3. Étape 3/6 - Mettre à jour Windows

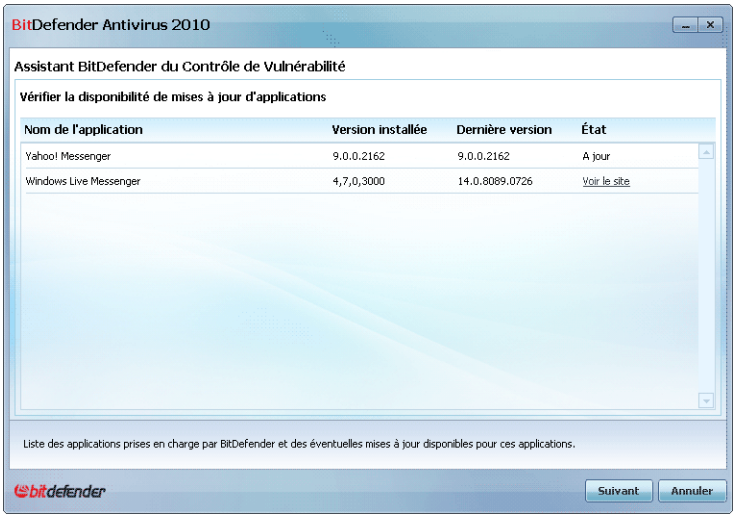

BitDefender Antivirus 2010
Assistant BitDefender du Contrôle de Vulnérabilité
Mises à jour Windows
Veuillez vérifier les mises à jour ci-dessous et les installer toutes ou utiliser le système de Mise à jour Windows Update pour choisir laquelle installer.
Installer les mises à jour système sélectionnées
Vérifier la disponibilité de mises à jour critiques Windows
Aucune mise à jour disponible dans cette catégorie.
Vérifier la disponibilité de mises à jour optionnelles Windows
Aucune mise à jour disponible dans cette catégorie.
Liste des mises à jour des applications Windows
bitdefender
Suivant
Annuler

Mises à jour Windows

Vous pouvez voir la liste des mises à jour Windows (critiques et non-critiques) qui ne sont pas installées actuellement sur votre ordinateur. Cliquez sur **Installer toutes les mises à jour système** pour installer toutes les mises à jour disponibles.

Cliquez sur **Suivant**.

11.3.4. Étape 4/6 - Mettre à jour les applications

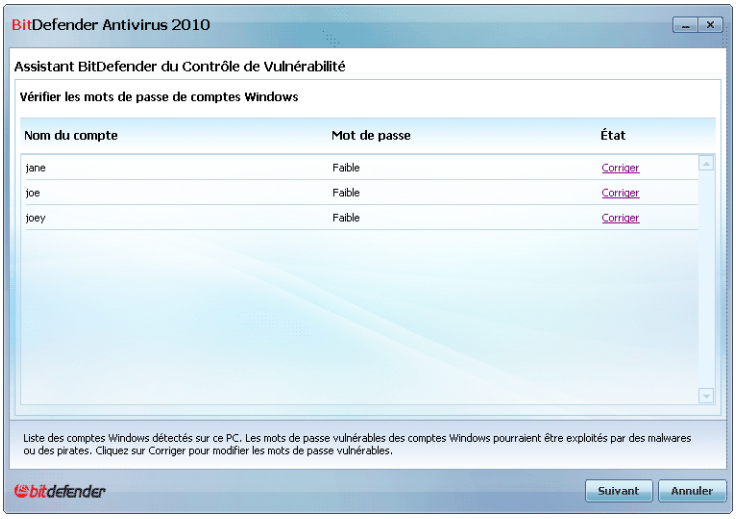


Applications

Vous pouvez voir la liste des applications vérifiées par BitDefender et savoir si ces dernières sont à jour. Si une application n'est pas à jour, cliquez sur le lien fourni pour télécharger la dernière version.

Cliquez sur **Suivant**.

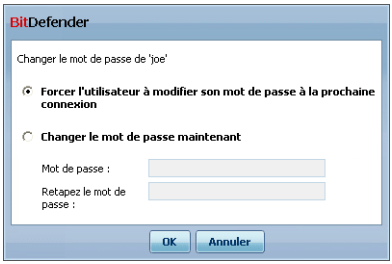
11.3.5. Étape 5/6 - Modifier les mots de passe vulnérables



Mots de passe utilisateur

Vous pouvez voir une liste des comptes utilisateur Windows configurés sur votre ordinateur ainsi que le niveau de protection que leur mot de passe respectif apportent. Un mot de passe peut être **sécurisé** (difficile à deviner) ou **vulnérable** (facile à deviner pour les personnes disposant de logiciels spécialisés).

Cliquez sur **Réparer** pour modifier les mots de passe vulnérables. Une nouvelle fenêtre s'affiche.


BitDefender
Changer le mot de passe de 'joe'
Forcer l'utilisateur à modifier son mot de passe à la prochaine connexion
Changer le mot de passe maintenant
Mot de passe :
Retapez le mot de passe :
OK
Annuler

Modifier le mot de passe

Choisir la méthode à utiliser pour régler ce problème :

- **Forcer l'utilisateur à modifier son mot de passe à la prochaine connexion.** BitDefender demandera à l'utilisateur de modifier son mot de passe lors de sa prochaine connexion à Windows
- **Modifier le mot de passe utilisateur.** Vous devez saisir le nouveau mot de passe dans les champs de modification. N'oubliez pas d'informer l'utilisateur du changement de mot de passe.

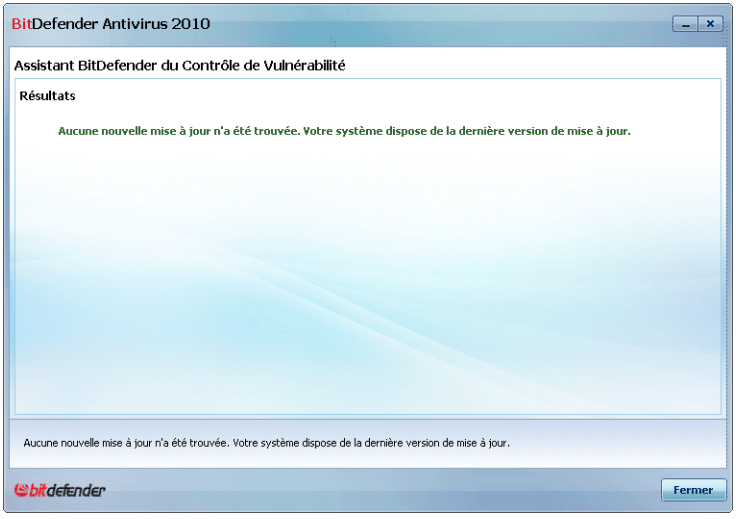
Note

Pour avoir un mot de passe Fort, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @). Vous pouvez rechercher sur Internet plus d'informations et de conseils sur la création de mots de passe sécurisés.

Cliquez sur **OK** pour changer le mot de passe.

Cliquez sur **Suivant**.

11.3.6. Étape 6/6 - Voir les résultats


BitDefender Antivirus 2010
Assistant BitDefender du Contrôle de Vulnérabilité
Résultats
Aucune nouvelle mise à jour n'a été trouvée. Votre système dispose de la dernière version de mise à jour.
Aucune nouvelle mise à jour n'a été trouvée. Votre système dispose de la dernière version de mise à jour.
bitdefender
Fermer

Résultats

Cliquez sur **Fermer**.

Mode Intermédiaire

12. État

L'onglet Tableau de Bord fournit des informations au sujet de l'état de sécurité de votre ordinateur et vous permet de corriger les problèmes en attente.

BitDefender Antivirus 2010 - Version d'évaluation
Configuration
TABLEAU DE BORD
ANTIVIRUS
ANTIPHISHING
VULNÉRABILITÉS
RÉSEAU
État de sécurité
Profil d'utilisation: Personnalisé
Mettre à jour
ATTENTION : 5 problèmes affectent l'état de sécurité de ce PC.
Tout corriger
Détails
ANTIVIRUS
ALERTE CRITIQUE - 1 problème en attente
ANTIPHISHING
PROTÉGÉ - Aucun problème
VULNÉRABILITÉS
ALERTE CRITIQUE - 4 problèmes en attente
RÉSEAU
ALERTE CRITIQUE - Des problèmes de sécurité affectent les ordinateurs de votre réseau
Le module Tableau de bord affiche l'état de sécurité du produit ainsi que des liens vers les principaux modules du produit.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

État

Le tableau de bord se compose des sections suivantes :

- **État Global** -Indique le nombre de problèmes affectant votre ordinateur et vous aide à les corriger. S'il y a des problèmes en attente, vous verrez un **cercle rouge avec un point d'exclamation** et le bouton **Tout Corriger**. Cliquez sur ce bouton pour lancer l'Assistant de Correction des problèmes.
- **Détail de l'état** - Indique l'état de chaque module principal à l'aide de phrases claires et avec l'une des icônes suivantes :

  Cercle vert coché : Aucun problème n'affecte l'état de sécurité. Votre ordinateur et vos données sont protégés.

  Cercle gris avec un point d'exclamation : L'activité des composants de ce module n'est pas surveillée. Il n'y a donc pas d'informations disponibles au sujet de leur état de sécurité. Il peut y avoir des problèmes spécifiques liés à ce module.

  Cercle rouge avec un point d'exclamation : Des problèmes affectent la sécurité de votre système. D'importants problèmes requièrent votre attention

immédiate. Des problèmes non critiques devraient également être réglés dès que possible.

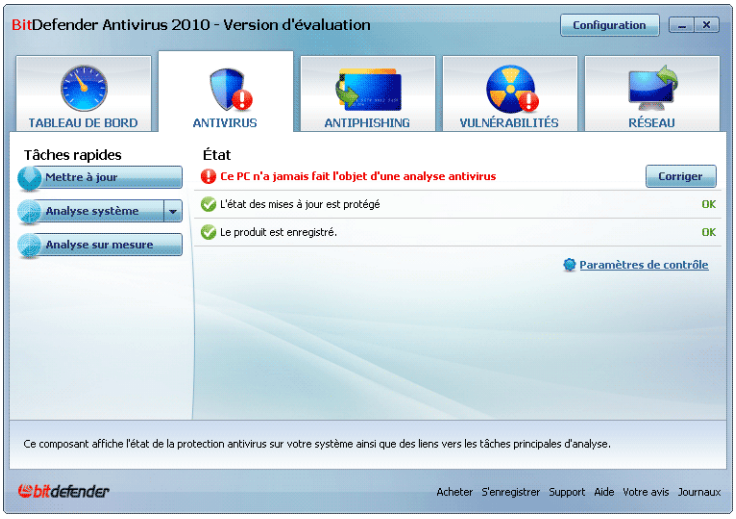
Cliquez sur le nom d'un module pour afficher plus de détails sur son état et configurer les paramètres de contrôle pour ses composants.

- **Profil d'Utilisation** - Indique le profil d'utilisation sélectionné et propose un lien vers une tâche adaptée à ce profil :
  - Lorsque le profil **Standard** est sélectionné, le bouton **Analyser** permet de réaliser une Analyse du Système en utilisant l'Assistant d'Analyse Antivirus. Tout le système sera analysé, sauf les archives. Avec la configuration par défaut, l'analyse recherche tous les types de malwares à l'exception des rootkits.
  - Lorsque le profil **Gamer** est sélectionné, le bouton **Activer/Désactiver le Mode Jeu** vous permet d'activer/de désactiver le Mode Jeu. Le Mode Jeu modifie temporairement les paramètres de protection afin de minimiser leur impact sur les performances du système.
  - Lorsque le profil **Personnalisé** est sélectionné, le bouton **Mettre à jour** lance immédiatement une mise à jour. Une nouvelle fenêtre apparaît affichant l'état de la mise à jour.

  Si vous souhaitez changer de profil ou modifier celui que vous utilisez en ce moment, cliquez sur le profil et suivez l'assistant de configuration.

13. Antivirus

BitDefender comporte un module Antivirus qui vous permet de maintenir votre BitDefender à jour et votre système protégé contre les virus. Pour accéder au module Antivirus, cliquez sur l'onglet **Antivirus**.



Antivirus

Le module Antivirus se compose de deux sections :

- **Zone d'état** - Affiche l'état de tous les composants de sécurité surveillés et vous permet de choisir les composants à surveiller.
- **Tâches Rapides** - Vous trouverez dans cette rubrique des liens vers les principales tâches de sécurité : mise à jour, analyse de mes documents, analyse du système, analyse approfondie et analyse personnalisée.

13.1. Zone d'état

La zone d'état vous permet de voir la liste complète des composants du module de sécurité et leur état actuel. En surveillant chaque module de sécurité, BitDefender vous prévient lorsque vous réalisez une configuration pouvant affecter la sécurité de votre ordinateur ou lorsque vous oubliez d'effectuer des tâches importantes.

L'état actuel d'un composant est indiqué en utilisant des phrases explicites et l'une des icônes suivantes :

Cercle vert coché : Aucun problème n'affecte le composant.

Cercle rouge avec un point d'exclamation : Problèmes affectent le composant.

Les phrases décrivant des problèmes sont en rouge. Cliquez simplement sur le bouton **Corriger** correspondant à une phrase pour corriger le problème signalé. Si un problème de sécurité n'a pas pu être directement résolu, suivez les instructions de l'assistant.

13.1.1. Configuration des paramètres de contrôle

Pour sélectionner les composants que BitDefender devrait surveiller, cliquez sur **Configurer le système de Contrôle d'état** et cochez la case **Activer les alertes** pour les fonctionnalités que vous souhaitez surveiller.

Important

Pour assurer une protection complète à votre système activez le contrôle pour tous les composants et corrigez tous les problèmes signalés.

L'état des composants de sécurité suivants peut être contrôlé par BitDefender :

- **Antivirus** - BitDefender surveille d'état des deux composants de la fonctionnalité Antivirus : la protection en temps réel et l'analyse à la demande. Les problèmes les plus fréquents pour ce composant sont répertoriés dans le tableau suivant.

Problème	Description
La protection en temps réel est désactivée	Les fichiers ne sont pas analysés lorsqu'un accès se produit (par vous ou par une application s'exécutant sur ce système).
Ce PC n'a jamais fait l'objet d'une analyse antivirus	Aucune analyse à la demande n'a été réalisée pour vérifier que les fichiers de votre ordinateur ne contiennent pas de malwares.
La dernière analyse du système que vous avez lancée a été arrêtée avant la fin	Une analyse complète du système a été lancée mais n'a pas été terminée.
Antivirus dans un état critique	La protection en temps réel est désactivée et une analyse du système doit être réalisée.

- **Mise à jour** - BitDefender vérifie que les signatures de codes malveillants sont à jour. Les problèmes les plus fréquents pour ce composant sont répertoriés dans le tableau suivant.

Problème	Description
La Mise à jour Automatique est désactivée	Les signatures de codes malveillants de votre produit BitDefender ne sont pas mises à jour automatiquement et régulièrement.
La mise à jour n'a pas été faite depuis x jours	Les signatures de codes malveillants de votre produit BitDefender ne sont pas à jour.

13.2. Tâches rapides

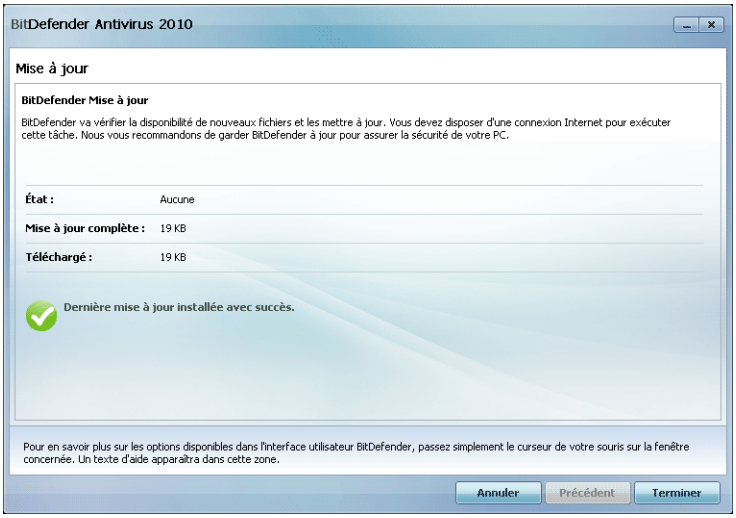
Vous trouverez ici des liens vers les tâches de sécurité les plus importantes :

- **Mettre à jour** - effectue une mise à jour immédiate.
- **Analyse du Système** - lance une analyse complète de votre ordinateur (hors archives). Pour des tâches d'analyse à la demande supplémentaires, cliquez sur le de ce bouton et sélectionnez une tâche d'analyse différente : Analyse de Mes Documents ou Analyse approfondie du Système.
- **Analyse Personnalisée** - lance un assistant qui vous permet de créer et d'exécuter une tâche d'analyse personnalisée.

13.2.1. Mettre à jour BitDefender

Chaque jour, de nouveaux codes malveillants sont détectés et identifiés. C'est pourquoi il est très important que BitDefender soit à jour dans les signatures de codes malveillants.

Par défaut, BitDefender recherche des mises à jour au démarrage de votre PC puis **chaque heure** après cela. Cependant, si vous voulez mettre à jour BitDefender, cliquez juste sur **Mettre à jour**. Le processus de mise à jour débutera et la fenêtre suivante apparaîtra immédiatement :


BitDefender Antivirus 2010
Mise à jour
BitDefender Mise à jour
BitDefender va vérifier la disponibilité de nouveaux fichiers et les mettre à jour. Vous devez disposer d'une connexion Internet pour exécuter cette tâche. Nous vous recommandons de garder BitDefender à jour pour assurer la sécurité de votre PC.
État :
Aucune
Mise à jour complète :
19 KB
Téléchargé :
19 KB
Dernière mise à jour installée avec succès.
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Terminer

Mettre à jour BitDefender

Dans cette fenêtre, vous pouvez voir le statut du processus de mise à jour.

Le processus de mise à jour est exécuté à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, le processus de mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.

Si vous voulez fermer cette fenêtre, cliquez simplement sur **Annuler**. Cependant, cela n'arrêtera pas le processus de mise à jour.

Note
Si vous êtes connecté à Internet via une connexion RTC (ou RNIS), nous vous conseillons de prendre l'habitude d'utiliser régulièrement les mises à jour à la demande.

Redémarrez votre ordinateur si nécessaire. En cas de mise à jour majeure, il vous sera demandé de redémarrer votre ordinateur. Cliquez sur **Redémarrer** pour redémarrer immédiatement votre système.

Si vous souhaitez redémarrer votre système plus tard, cliquez juste sur **OK**. Nous vous recommandons de redémarrer votre système dès que possible.

13.2.2. Analyser avec BitDefender

Pour rechercher la présence de malwares sur votre ordinateur, exécutez une tâche d'analyse particulière en cliquant sur le bouton correspondant ou sélectionnez-la

dans le menu déroulant. Le tableau ci-dessous affiche la liste des tâches disponibles, ainsi que leur description :

Tâche	Description
Analyse du Système	Analyse l'ensemble du système, mis à part les archives. Dans la configuration par défaut, l'analyse recherche tous les types de malwares à l'exception des rootkits.
Analyse de Mes documents	Utilisez cette tâche pour analyser les dossiers importants de l'utilisateur actuel: `Mes documents`, `Bureau` et `Démarrage`. Celle assurera la sécurité de vos documents et de votre bureau, ainsi que le contrôle des applications se lançant au démarrage.
Analyse approfondie du système	Analyse l'ensemble du système. La configuration par défaut permet d'analyser tous les types de codes malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse personnalisée	Utilisez cette tâche pour définir des fichiers et dossiers spécifiques à analyser.

Note

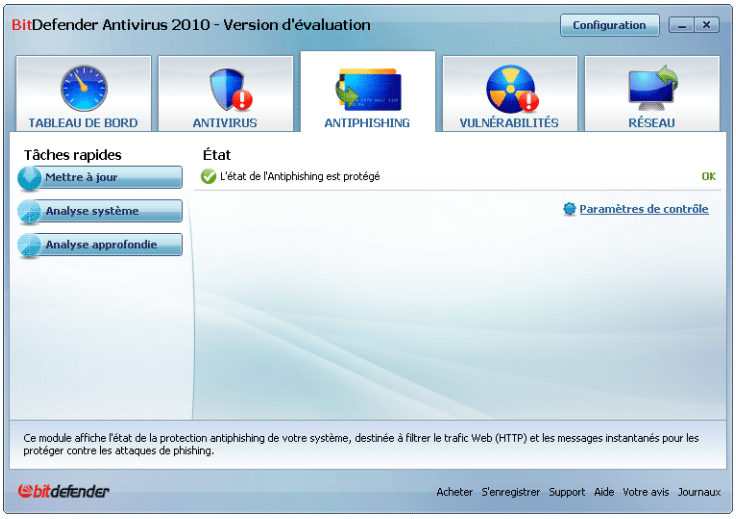
Sachant que les tâches d'**Analyse approfondie du système** et **d'Analyse complète du système** analysent l'intégralité du système, l'analyse peut prendre un certain temps. C'est pourquoi nous vous recommandons d'exécuter ces tâches en priorité faible ou, si cela est possible, lorsque votre système est inactif.

Lorsque vous lancez une analyse du système, une analyse approfondie du système ou une analyse de Mes Documents, l'assistant d'Analyse Antivirus apparaît. Suivez cette procédure en trois étapes pour effectuer le processus d'analyse: Pour plus d'informations sur cet assistant, veuillez consulter « *Assistant d'analyse antivirus* » (p. 55).

L'Assistant d'Analyse Personnalisée vous guidera au long du processus d'analyse lorsque vous réaliserez une Analyse Personnalisée. Suivez cette procédure en six étapes pour analyser des fichiers ou des dossiers spécifiques. Pour plus d'informations sur cet assistant, reportez-vous à « *Assistant d'Analyse Personnalisée* » (p. 60).

14. Antispyware

BitDefender comporte un module Antiphishing qui vérifie que toutes les pages auxquelles vous accédez avec Internet Explorer ou Firefox sont sûres. Pour accéder au module Antiphishing, cliquez sur l'onglet **Antiphishing**.



Antispyware

Le module Antiphishing se compose de deux sections :

- **Zone d'état** - Affiche l'état du module Antiphishing et permet d'activer/de désactiver le contrôle de l'activité de ce module.
- **Tâches Rapides** - Vous trouverez dans cette rubrique des liens vers d'importantes tâches de sécurité : mise à jour, analyse du système, et analyse approfondie du système.

14.1. Zone d'état

L'état actuel d'un composant est indiqué en utilisant des phrases explicites et l'une des icônes suivantes :

Cercle vert coché : Aucun problème n'affecte le composant.

Cercle rouge avec un point d'exclamation : Problèmes affectent le composant.

Les phrases décrivant des problèmes sont en rouge. Cliquez simplement sur le bouton **Corriger** correspondant à une phrase pour corriger le problème signalé.

Le problème le plus fréquent pour ce module est **Antiphishing désactivé**. Cela signifie que l'Antiphishing n'est pas activé pour une ou plusieurs application(s) prise(s) en charge : Internet Explorer, Mozilla Firefox, Yahoo! Messenger et Windows Live Messenger.

14.2. Tâches rapides

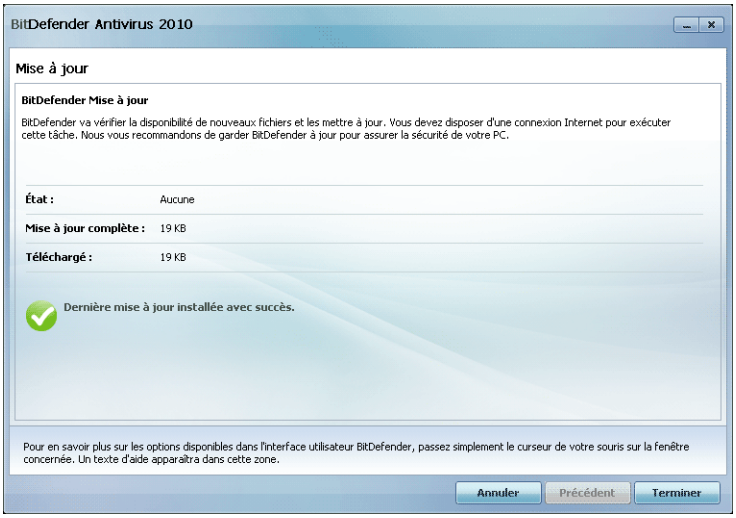
Vous trouverez ici des liens vers les tâches de sécurité les plus importantes :

- **Mettre à jour** - effectue une mise à jour immédiate.
- **Analyse du Système** -lance une analyse complète de votre ordinateur (hors archives).
- **Analyse approfondie du système** -lance une analyse approfondie de votre ordinateur (y compris des archives).

14.2.1. Mettre à jour BitDefender

Chaque jour, de nouveaux codes malveillants sont détectés et identifiés. C'est pourquoi il est très important que BitDefender soit à jour dans les signatures de codes malveillants.

Par défaut, BitDefender recherche des mises à jour au démarrage de votre PC puis **chaque heure** après cela. Cependant, si vous voulez mettre à jour BitDefender, cliquez juste sur **Mettre à jour**. Le processus de mise à jour débutera et la fenêtre suivante apparaîtra immédiatement :


BitDefender Antivirus 2010
Mise à jour
BitDefender Mise à jour
BitDefender va vérifier la disponibilité de nouveaux fichiers et les mettre à jour. Vous devez disposer d'une connexion Internet pour exécuter cette tâche. Nous vous recommandons de garder BitDefender à jour pour assurer la sécurité de votre PC.
État :
Aucune
Mise à jour complète :
19 KB
Téléchargé :
19 KB
Dernière mise à jour installée avec succès.
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Terminer

Mettre à jour BitDefender

Dans cette fenêtre, vous pouvez voir le statut du processus de mise à jour.

Le processus de mise à jour est exécuté à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, le processus de mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.

Si vous voulez fermer cette fenêtre, cliquez simplement sur **Annuler**. Cependant, cela n'arrêtera pas le processus de mise à jour.

Note
Si vous êtes connecté à Internet via une connexion RTC (ou RNIS), nous vous conseillons de prendre l'habitude d'utiliser régulièrement les mises à jour à la demande.

Redémarrez votre ordinateur si nécessaire. En cas de mise à jour majeure, il vous sera demandé de redémarrer votre ordinateur. Cliquez sur **Redémarrer** pour redémarrer immédiatement votre système.

Si vous souhaitez redémarrer votre système plus tard, cliquez juste sur **OK**. Nous vous recommandons de redémarrer votre système dès que possible.

14.2.2. Analyser avec BitDefender

Pour rechercher la présence de malwares sur votre ordinateur, exécutez une tâche d'analyse particulière en cliquant sur le bouton correspondant ou sélectionnez-la

dans le menu déroulant. Le tableau ci-dessous affiche la liste des tâches disponibles, ainsi que leur description :

Tâche	Description
Analyse du Système	Analyse l'ensemble du système, mis à part les archives. Dans la configuration par défaut, l'analyse recherche tous les types de malwares à l'exception des rootkits.
Analyse approfondie du système	Analyse l'ensemble du système. La configuration par défaut permet d'analyser tous les types de codes malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.

Note

Sachant que les tâches d'**Analyse approfondie du système** et **d'Analyse complète du système** analysent l'intégralité du système, l'analyse peut prendre un certain temps. C'est pourquoi nous vous recommandons d'exécuter ces tâches en priorité faible ou, si cela est possible, lorsque votre système est inactif.

Lorsque vous lancez une analyse du système, ou une analyse approfondie du système, l'assistant d'Analyse Antivirus apparaît. Suivez cette procédure en trois étapes pour effectuer le processus d'analyse: Pour plus d'informations sur cet assistant, veuillez consulter « *Assistant d'analyse antivirus* » (p. 55).

15. Vulnérabilité

BitDefender comporte un module Vulnérabilité qui vous permet de maintenir les logiciels essentiels pour votre PC constamment à jour. Pour surveiller et corriger les vulnérabilités de votre système, cliquez sur l'onglet **Vulnérabilité**.

BitDefender Antivirus 2010 - Version d'évaluation
Configuration
TABLEAU DE BORD
ANTIVIRUS
ANTIPHISHING
VULNÉRABILITÉS
RÉSEAU
Tâches rapides
État
Vulnérabilité
L'état de l'Analyse de Vulnérabilité est critique (4 problèmes)
Corriger
Paramètres de contrôle
Ce composant affiche l'état du module de Contrôle de Vulnerabilité, conçu pour vérifier que le système d'exploitation et les applications installés sur ce PC sont à jour et que les mots de passe des comptes Windows ne peuvent pas être contournés.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

Vulnérabilité

Le module Vulnérabilité comporte deux sections :

- **Zone d'état** - Affiche l'état du module de Contrôle de Vulnérabilité et permet d'activer/de désactiver le contrôle de l'activité de ce module.
- **Tâches Rapides** - Vous trouverez dans cette rubrique un lien vers l'Assistant du Contrôle de Vulnérabilité.

15.1. Zone d'état

L'état actuel d'un composant est indiqué en utilisant des phrases explicites et l'une des icônes suivantes :

Cercle vert coché : Aucun problème n'affecte le composant.

Cercle rouge avec un point d'exclamation : Problèmes affectent le composant.

Les phrases décrivant des problèmes sont en rouge. Cliquez simplement sur le bouton **Corriger** ou **Installer** correspondant à une phrase pour corriger le problème signalé.

Les problèmes les plus fréquents pour ce composant sont répertoriés dans le tableau suivant.

État	Description
Contrôle de Vulnérabilité désactivé	BitDefender ne vérifie pas d'éventuelles vulnérabilités concernant des mises à jour Windows ou d'applications manquantes ou des mots de passe non sécurisés.
De multiples vulnérabilités ont été détectées	BitDefender a trouvé des mises à jour Windows/d'applications manquantes et/ou des mots de passe non sécurisés.
Mises à jour critiques de Microsoft	Des mises à jour critiques de Microsoft sont disponibles mais n'ont pas été installées.
Autres mises à jour de Microsoft	Des mises à jour non critiques de Microsoft sont disponibles mais n'ont pas été installées.
Mises à jour automatiques de Windows désactivées	Les mises à jour de sécurité Windows ne sont pas installées automatiquement lorsqu'elles deviennent disponibles.
`Application` (non à jour)	Une nouvelle version de l'`Application` est disponible mais n'a pas été installée.
`Utilisateur` (Mot de passe non sécurisé)	Un mot de passe utilisateur peut être facilement découvert par des personnes mal intentionnées disposant de logiciels spécialisés.

15.2. Tâches rapides

Il n'y a qu'une tâche disponible :

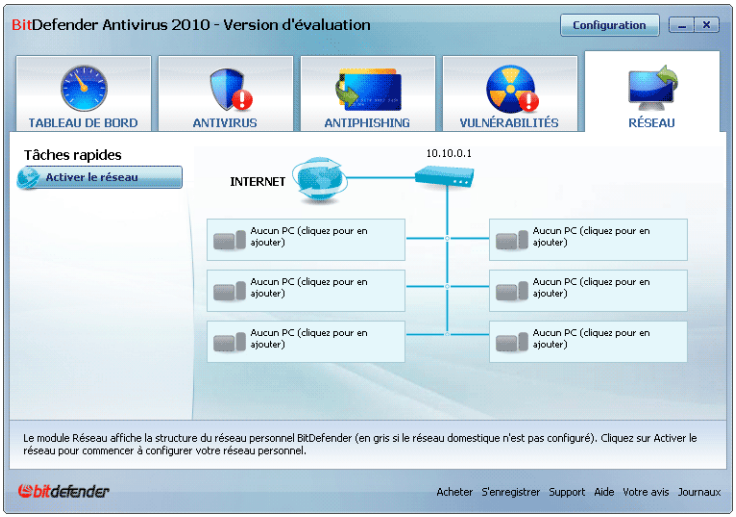
- **Analyse de Vulnérabilité** -lance un assistant qui recherche les vulnérabilités de votre système et vous aide à les corriger.

L'analyse de vulnérabilité vérifie les mises à jour Microsoft Windows et Microsoft Windows Office et les mots de passe d'accès à vos comptes Microsoft Windows afin de veiller à ce que votre système d'exploitation soit à jour et non vulnérable au contournement de mot de passe.

Pour rechercher les vulnérabilités de votre ordinateur, cliquez sur **Analyse de Vulnérabilité** et suivez l'« *Assistant du Contrôle de Vulnérabilité* » (p. 67).

16. Réseau

Le module Réseau vous permet de gérer les produits BitDefender installés sur tous les ordinateurs de votre foyer à partir d'un seul et même ordinateur. Pour accéder au module Réseau, cliquez sur l'onglet **Réseau**.


BitDefender Antivirus 2010 - Version d'évaluation
Configuration
TABLEAU DE BORD
ANTIVIRUS
ANTIPHISHING
VULNÉRABILITÉS
RÉSEAU
Tâches rapides
Activer le réseau
INTERNET
10.10.0.1
Aucun PC (cliquez pour en ajouter)
Aucun PC (cliquez pour en ajouter)
Aucun PC (cliquez pour en ajouter)
Aucun PC (cliquez pour en ajouter)
Aucun PC (cliquez pour en ajouter)
Aucun PC (cliquez pour en ajouter)
Le module Réseau affiche la structure du réseau personnel BitDefender (en gris si le réseau domestique n'est pas configuré). Cliquez sur Activer le réseau pour commencer à configurer votre réseau personnel.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

Réseau

Vous devez suivre ces étapes pour pouvoir gérer les produits BitDefender installés sur tous les ordinateurs de votre foyer :

1. Rejoindre le réseau domestique BitDefender via votre ordinateur. Rejoindre le réseau consiste à configurer un mot de passe d'administration pour la gestion du réseau domestique.
2. Allumez chaque ordinateur que vous voulez gérer et rejoignez le réseau à partir de ceux-ci (en saisissant le mot de passe).
3. Revenez sur votre ordinateur et ajoutez les ordinateurs que vous voulez gérer.

16.1. Tâches rapides

Au début, seul un bouton est disponible.

- **Activer le Réseau** - vous permet de définir le mot de passe réseau, et donc de créer et de rejoindre un réseau.

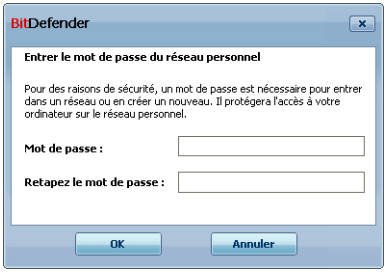
Après avoir rejoint le réseau, plusieurs autres boutons sont accessibles.

- **Désactiver le réseau** - vous permet de quitter le réseau.
- **Ajouter un PC** - vous permet d'ajouter des ordinateurs à votre réseau.
- **Analyser tout** - vous permet d'analyser en une seule opération l'ensemble des ordinateurs gérés.
- **Tout mettre à jour** vous permet de mettre à jour en une seule opération l'ensemble des ordinateurs gérés.
- **Enregistrer tout** vous permet d'enregistrer en une seule opération l'ensemble des ordinateurs gérés.

16.1.1. Rejoindre le réseau BitDefender

Procédez comme suit pour rejoindre le réseau domestique BitDefender :

1. Cliquez sur **Activer le Réseau**. Vous serez invité à définir le mot de passe de gestion de réseau domestique.


BitDefender
Entrer le mot de passe du réseau personnel
Pour des raisons de sécurité, un mot de passe est nécessaire pour entrer dans un réseau ou en créer un nouveau. Il protégera l'accès à votre ordinateur sur le réseau personnel.
Mot de passe :
Retapez le mot de passe :
OK
Annuler

Définir le mot de passe

2. Entrez le même mot de passe dans chacun des champs de saisie.
3. Cliquez sur **OK**.

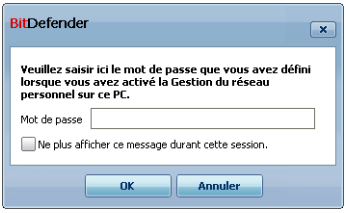
Vous pouvez voir apparaître le nom de l'ordinateur sur la carte réseau.

16.1.2. Ajout d'ordinateurs au réseau BitDefender

Avant de pouvoir ajouter un ordinateur au réseau domestique BitDefender, vous devez définir le mot de passe de gestion de réseau domestique BitDefender sur l'ordinateur à ajouter.

Procédez comme suit pour ajouter un ordinateur au réseau domestique BitDefender :

1. Cliquez sur **Ajouter un PC**. Vous serez invité à saisir le mot de passe local de gestion de réseau domestique.


BitDefender
Veuillez saisir ici le mot de passe que vous avez défini lorsque vous avez activé la Gestion du réseau personnel sur ce PC.
Mot de passe
Ne plus afficher ce message durant cette session.
OK
Annuler

Saisir le mot de passe

2. Tapez le mot de passe de gestion de réseau domestique et cliquez sur **OK**. Une nouvelle fenêtre s'affiche.

Ajouter un PC

Vous pouvez voir à l'écran la liste des ordinateurs rattachés au réseau. La signification des icônes est la suivante :

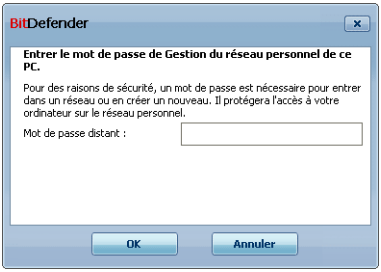
Indique un ordinateur en ligne sans aucun produit BitDefender installé.

Indique un ordinateur en ligne avec BitDefender installé.

Indique un ordinateur hors connexion avec BitDefender installé.

3. Choisissez une des possibilités suivantes :
   - Sélectionnez dans la liste le nom de l'ordinateur à ajouter.
   - Tapez l'adresse IP ou le nom de l'ordinateur à ajouter dans le champ correspondant.

4. Cliquez sur **Ajouter**. Vous serez invité à saisir le mot de passe de gestion de réseau domestique de l'ordinateur concerné.


BitDefender
Entrer le mot de passe de Gestion du réseau personnel de ce PC.
Pour des raisons de sécurité, un mot de passe est nécessaire pour entrer dans un réseau ou en créer un nouveau. Il protégera l'accès à votre ordinateur sur le réseau personnel.
Mot de passe distant :
OK
Annuler

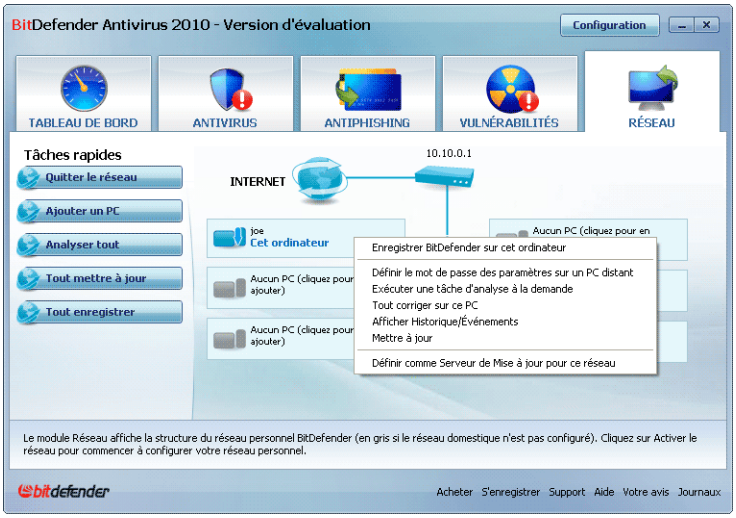
Authentification

5. Tapez le mot de passe de gestion de réseau domestique défini sur l'ordinateur concerné.
6. Cliquez sur **OK**. Si vous avez spécifié le bon mot de passe, le nom de l'ordinateur sélectionné apparaît sur la carte réseau.

Note
Vous pouvez ajouter jusqu'à cinq ordinateurs sur la carte réseau.

16.1.3. Gestion du réseau BitDefender

Une fois votre réseau domestique BitDefender créé, vous pouvez gérer l'ensemble des produits BitDefender à partir d'un seul et même ordinateur.



Carte réseau

Si vous déplacez le curseur sur un ordinateur de la carte réseau, vous pouvez consulter quelques informations le concernant (nom, adresse IP, nombre de problèmes affectant la sécurité du système, état d'enregistrement de BitDefender).

Si vous faites un clic-droit sur un ordinateur présent sur la carte du réseau, vous pourrez voir les tâches administratives que vous pouvez lancer sur cet ordinateur distant.

- **Retirer le PC du réseau personnel**

  Vous permet de retirer un PC du réseau.

- **Enregistrer BitDefender sur cet ordinateur**

  Vous permet d'enregistrer BitDefender sur cet ordinateur en entrant une clé de licence.

- **Définir un mot de passe des paramètres sur un PC distant**

  Vous permet de créer un mot de passe pour limiter l'accès aux paramètres de BitDefender sur ce PC.

- **Lancer une tâche d'analyse à la demande**

  Vous permet de lancer une analyse à la demande sur un ordinateur distant. Vous pouvez réaliser l'une des tâches d'analyse suivantes : Analyse de Mes Documents, Analyse du Système ou Analyse Approfondie du Système.

- **Corriger tous les problèmes de ce PC**

Vous permet de corriger les problèmes qui affectent la sécurité de cet ordinateur à l'aide de l'assistant Tout corriger.

- **Afficher Historique/Événements**

  Vous permet d'accéder au module **Historique&Événements** du produit BitDefender installé sur cet ordinateur.

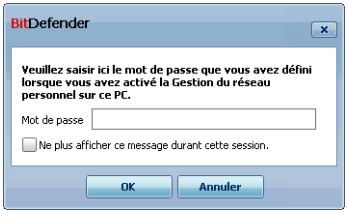
- **Mettre à jour**

  Lance le processus de Mise à jour du produit BitDefender installé sur cet ordinateur.

- **Définir comme Serveur de Mise à Jour pour ce réseau**

  Vous permet de définir cet ordinateur comme serveur de mise à jour pour tous les produits BitDefender installés sur les ordinateurs de ce réseau. Utiliser cette option réduira le trafic Internet car seul un ordinateur du réseau se connectera à Internet pour télécharger des mises à jour.

Avant de lancer une tâche sur un ordinateur spécifique, vous serez invité à saisir le mot de passe local de gestion de réseau domestique.


BitDefender
Veuillez saisir ici le mot de passe que vous avez défini lorsque vous avez activé la Gestion du réseau personnel sur ce PC.
Mot de passe
Ne plus afficher ce message durant cette session.
OK
Annuler

Saisir le mot de passe

Tapez le mot de passe de gestion de réseau domestique et cliquez sur **OK**.

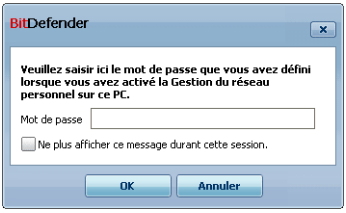
Note

Si vous prévoyez de lancer plusieurs tâches, il peut s'avérer utile de sélectionner l'option **Ne plus afficher ce message durant cette session**. En sélectionnant cette option, vous n'aurez plus à saisir le mot de passe pour la session en cours.

16.1.4. Analyse de tous les ordinateurs

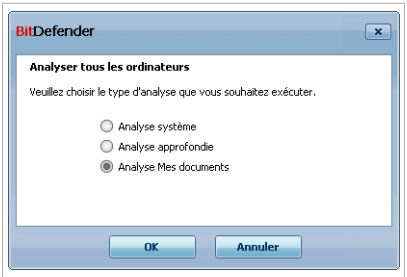
Procédez comme suit pour analyser tous les ordinateurs gérés :

1. Cliquez sur **Analyser tout**. Vous serez invité à saisir le mot de passe local de gestion de réseau domestique.


BitDefender
Veuillez saisir ici le mot de passe que vous avez défini lorsque vous avez activé la Gestion du réseau personnel sur ce PC.
Mot de passe
Ne plus afficher ce message durant cette session.
OK
Annuler

Saisir le mot de passe

2. Sélectionnez un type d'analyse.
   - **Analyse du Système** -lance une analyse complète de votre ordinateur (hors archives).
   - **Analyse approfondie du système** -lance une analyse approfondie de votre ordinateur (y compris des archives).
   - **Analyse de Mes documents**" – lance une analyse rapide de vos documents et paramètres.



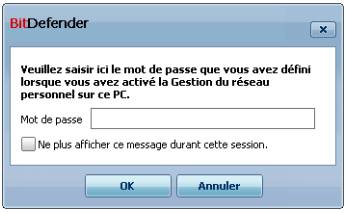
Sélectionner le type d'analyse

3. Cliquez sur **OK**.

16.1.5. Mise à jour de tous les ordinateurs

Procédez comme suit pour mettre à jour tous les ordinateurs gérés :

1. Cliquez sur **Tout mettre à jour**. Vous serez invité à saisir le mot de passe local de gestion de réseau domestique.


BitDefender
Veuillez saisir ici le mot de passe que vous avez défini lorsque vous avez activé la Gestion du réseau personnel sur ce PC.
Mot de passe
Ne plus afficher ce message durant cette session.
OK
Annuler

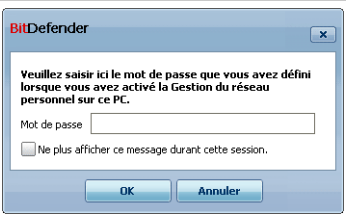
Saisir le mot de passe

2. Cliquez sur **OK**.

16.1.6. Enregistrement de tous les ordinateurs

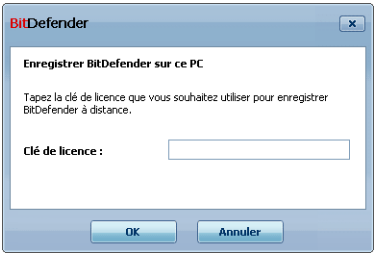
Procédez comme suit pour enregistrer tous les ordinateurs gérés :

1. Cliquez sur **Enregistrer tout**. Vous serez invité à saisir le mot de passe local de gestion de réseau domestique.


BitDefender
Veuillez saisir ici le mot de passe que vous avez défini lorsque vous avez activé la Gestion du réseau personnel sur ce PC.
Mot de passe
Ne plus afficher ce message durant cette session.
OK
Annuler

Saisir le mot de passe

2. Saisissez la clé avec laquelle vous voulez vous enregistrer.


BitDefender
Enregistrer BitDefender sur ce PC
Tapez la clé de licence que vous souhaitez utiliser pour enregistrer BitDefender à distance.
Clé de licence :
OK
Annuler

Tout enregistrer

3. Cliquez sur **OK**.

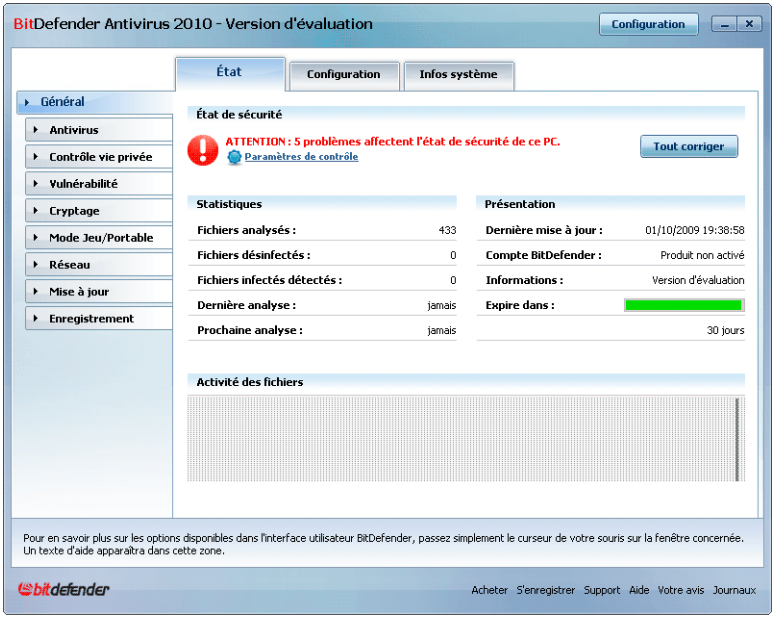
Mode Expert

17. Général

Le module Général donne des informations sur l'activité de BitDefender et sur le système. Vous pouvez également modifier le comportement global de BitDefender.

17.1. État

Pour savoir si des problèmes affectent votre ordinateur, et pour consulter les statistiques d'activité du produit et l'état de votre enregistrement, rendez-vous dans **Général>Tableau de bord** en Mode Expert.



État

Le tableau de bord se compose de plusieurs sections :

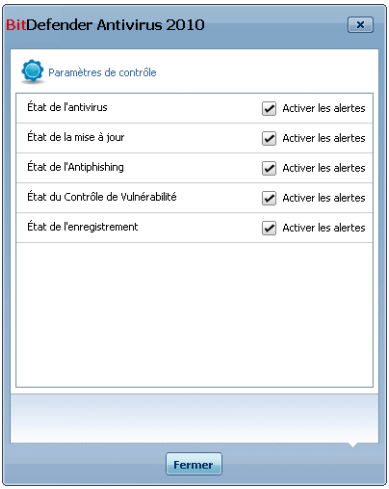
- **État Global** - vous informe des problèmes affectant la sécurité de votre ordinateur.
- **Statistiques** - Affiche des informations importantes sur l'activité de BitDefender.
- **Présentation** - Affiche l'état des mises à jour et des informations sur votre enregistrement et votre licence.

- **Activité des Fichiers** - Indique l'évolution du nombre d'objets analysés par l'Antimalware BitDefender. La hauteur de la barre indique l'intensité du trafic lors de l'intervalle de temps correspondant.

17.1.1. État global

Vous pouvez connaître ici le nombre de problèmes affectant la sécurité de votre ordinateur. Pour supprimer toutes les menaces, cliquez sur **Corriger tous les problèmes**. Cela lancera l'assistant Corriger tous les Problèmes.

Pour configurer quels modules seront surveillés par BitDefender Antivirus 2010, cliquez sur **Configurer le système de Contrôle d'état**. Une nouvelle fenêtre s'affichera :



Configurer le système de Contrôle d'état

Si vous voulez que BitDefender surveille un composant, cochez la case **Activer les alertes** pour ce composant. L'état des composants de sécurité suivants peut être contrôlé par BitDefender :

- **Antivirus** - BitDefender surveille l'état des deux composants du module Antivirus : la protection en temps réel et l'analyse à la demande. Les problèmes les plus fréquents pour ce composant sont répertoriés dans le tableau suivant.

Problème	Description
La protection en temps réel est désactivée	Les fichiers ne sont pas analysés lorsqu'un accès se produit (par vous ou par une application s'exécutant sur ce système).
Vous n'avez jamais analysé votre ordinateur pour rechercher des malwares	Aucune analyse à la demande n'a été réalisée pour vérifier que les fichiers de votre ordinateur ne contiennent pas de malwares.
La dernière analyse du système que vous avez lancée a été arrêtée avant la fin	Une analyse complète du système a été lancée mais n'a pas été terminée.
Antivirus dans un état critique	La protection en temps réel est désactivée et une analyse du système doit être réalisée.

- **Mise à jour** - BitDefender vérifie que les signatures de codes malveillants sont à jour. Les problèmes les plus fréquents pour ce composant sont répertoriés dans le tableau suivant.

Problème	Description
La Mise à jour Automatique est désactivée	Les signatures de codes malveillants de votre produit BitDefender ne sont pas mises à jour automatiquement et régulièrement.
La mise à jour n'a pas été faite depuis x jours	Les signatures de codes malveillants de votre produit BitDefender ne sont pas à jour.

- **Antiphishing** - BitDefender surveille l'état de la fonctionnalité Antiphishing. S'il n'est pas activé pour toutes les applications prises en charge, le problème **Antiphishing désactivé** sera signalé.
- **Contrôle de Vulnérabilité** - BitDefender surveille cette fonctionnalité. Le Contrôle de Vulnérabilité vous permet de savoir si vous avez besoin d'installer des mises à jour Windows, des mises à jour d'applications, ou si vous devez sécuriser des mots de passe.

  Les problèmes les plus fréquents pour ce composant sont répertoriés dans le tableau suivant.

État	Description
Contrôle de Vulnérabilité désactivé	BitDefender ne vérifie pas d'éventuelles vulnérabilités concernant des mises à jour Windows ou d'applications manquantes ou des mots de passe non sécurisés.
De multiples vulnérabilités ont été détectées	BitDefender a trouvé des mises à jour Windows/d'applications manquantes et/ou des mots de passe non sécurisés.
Mises à jour critiques de Microsoft	Des mises à jour critiques de Microsoft sont disponibles mais n'ont pas été installées.
Autres mises à jour de Microsoft	Des mises à jour non critiques de Microsoft sont disponibles mais n'ont pas été installées.
Mises à jour automatiques de Windows désactivées	Les mises à jour de sécurité Windows ne sont pas installées automatiquement lorsqu'elles deviennent disponibles.
`Application` (non à jour)	Une nouvelle version de l'`Application` est disponible mais n'a pas été installée.
`Utilisateur` (Mot de passe non sécurisé)	Un mot de passe utilisateur peut être facilement découvert par des personnes mal intentionnées disposant de logiciels spécialisés.

Important

Pour assurer une protection complète à votre système activez le contrôle pour tous les composants et corrigez tous les problèmes signalés.

17.1.2. Statistiques

Si vous voulez garder un œil sur l'activité de BitDefender, vous pouvez commencer par consulter la section Statistiques. Vous pouvez consulter les éléments suivants :

Elément	Description
Fichiers analysés	Indique le nombre de fichiers ayant fait l'objet d'une analyse antimalware lors de votre dernière analyse.
Fichiers désinfectés	Indique le nombre de fichiers désinfectés lors de votre dernière analyse.
Fichiers infectés détectés	Indique le nombre de fichiers infectés trouvés sur votre système lors de la dernière analyse.

Elément	Description
Dernière analyse du système	Indique à quel moment votre ordinateur a été analysé la dernière fois. Si la dernière analyse a eu lieu plus d'une semaine auparavant, veuillez analyser votre ordinateur le plus rapidement possible. Pour analyser l'ordinateur dans son entier, choisissez l'onglet **Antivirus**, Analyse antivirus, et lancez l'Analyse complète du système ou bien l'Analyse approfondie du système.
Prochaine analyse	Indique à quel moment votre ordinateur sera analysé de nouveau.

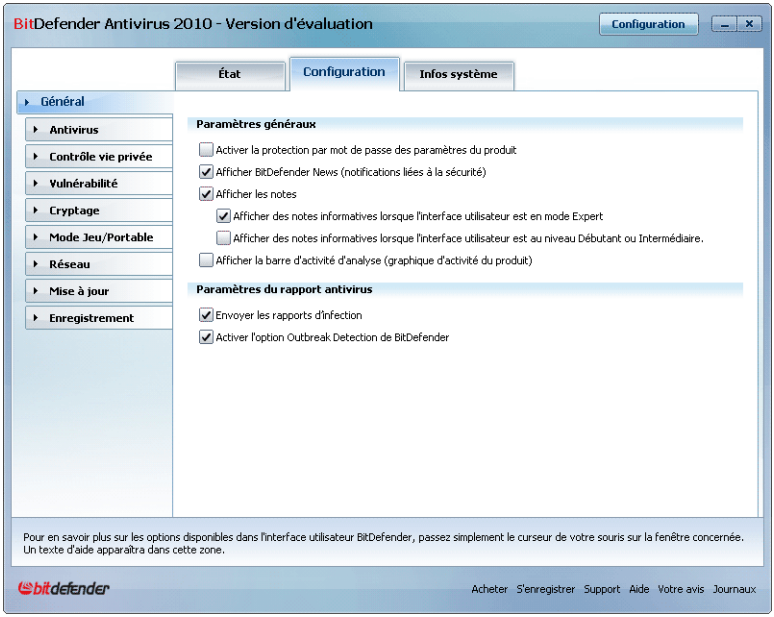
17.1.3. Présentation

Vous pouvez voir ici l'état de la mise à jour, l'état de votre compte, les informations d'enregistrement et de licence.

Elément	Description
Dernière mise à jour	Indique la date de la dernière mise à jour de votre produit BitDefender. Effectuez des mises à jour régulières pour avoir un système complètement protégé.
Compte BitDefender	Indique l'adresse e-mail que vous pouvez utiliser pour accéder à votre compte en ligne, afin de récupérer votre clé de licence BitDefender, si vous l'avez perdue, et de bénéficier du Support Technique BitDefender ainsi que d'autres services personnalisés. Vous devez créer un compte BitDefender pour activer votre produit. Pour plus d'informations sur le compte BitDefender, référez-vous à « *Enregistrement et Mon compte* » (p. 50).
Enregistrement	Indique le type et l'état de votre clé de licence. Pour conserver votre système à l'abri des menaces, vous devez renouveler la clé ou mettre à niveau BitDefender si votre clé a expiré.
Expire dans	Indique le nombre de jours avant l'expiration de la clé de licence. Si votre clé de licence expire dans les jours qui suivent, veuillez enregistrer le produit avec une nouvelle clé de licence. Pour acheter une clé de licence ou pour renouveler votre licence, cliquez sur le lien **Acheter/Renouveler**, situé en bas de la fenêtre.

17.2. Configuration

Pour configurer les paramètres généraux de BitDefender et gérer sa configuration, rendez-vous dans **Général>Paramètres** en Mode Expert.


BitDefender Antivirus 2010 - Version d'évaluation
Configuration
État
Configuration
Infos système
Général
Antivirus
Contrôle vie privée
Vulnérabilité
Cryptage
Mode Jeu/Portable
Réseau
Mise à jour
Enregistrement
Paramètres généraux
Activer la protection par mot de passe des paramètres du produit
Afficher BitDefender News (notifications liées à la sécurité)
Afficher les notes
Afficher des notes informatives lorsque l'interface utilisateur est en mode Expert
Afficher des notes informatives lorsque l'interface utilisateur est au niveau Débutant ou Intermédiaire.
Afficher la barre d'activité d'analyse (graphique d'activité du produit)
Paramètres du rapport antivirus
Envoyer les rapports d'infection
Activer l'option Outbreak Detection de BitDefender
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

Paramètres généraux

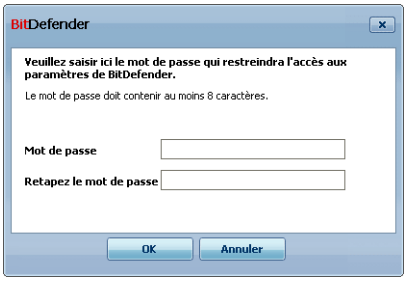
Vous pouvez dans cette rubrique paramétrer le fonctionnement de BitDefender. Par défaut, BitDefender est chargé au démarrage de Windows et se minimise automatiquement.

17.2.1. Paramètres généraux

- **Activer la protection par mot de passe pour les paramètres du produit** - permet de choisir un mot de passe afin de protéger la configuration de BitDefender.

  Note
  Si vous n'êtes pas le seul utilisateur avec des droits d'administrateur qui utilise cet ordinateur, il vous est recommandé de protéger vos paramètres BitDefender par un mot de passe.

  Si vous sélectionnez cette option, la fenêtre suivante apparaîtra :


BitDefender
Veuillez saisir ici le mot de passe qui restreindra l'accès aux paramètres de BitDefender.
Le mot de passe doit contenir au moins 8 caractères.
Mot de passe
Retapez le mot de passe
OK
Annuler

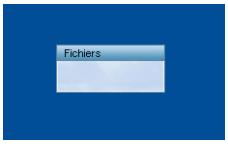
Entrer le mot de passe

Entrez le mot de passe dans le champ **Mot de passe**, re-saisissez le dans le champ **Resaisir le mot de passe** et cliquez sur **OK**.

Une fois le mot de passe paramétré, il vous sera demandé dès que vous voudrez changer les paramètres de BitDefender. Les autres administrateurs du système, s'il y en a, auront également à fournir le mot de passe pour changer les paramètres de BitDefender.

Important
Si vous avez oublié votre mot de passe vous devrez réinstaller partiellement le produit pour modifier la configuration de BitDefender.

- **Afficher BitDefender News (notifications liées à la sécurité)** - communique de temps en temps les notifications de sécurité relatives aux irruptions de virus envoyées par le serveur BitDefender.
- **Afficher des notes sur l'écran** - affiche des fenêtres de notifications sur l'état de votre produit. Vous pouvez configurer BitDefender pour qu'il affiche des pop-up lorsque l'interface est en Mode Débutant / Intermédiaire ou en Mode Expert.
- **Activer la barre d'analyse de l'activité (graphique de l'activité du produit)** - affiche la barre d'analyse de l'activité à chaque fois que vous démarrez Windows.. Décochez cette case si vous ne voulez plus que la barre d'analyse de l'activité s'affiche.



Barre de l'activité d'analyse

Note
Seul le compte utilisateur Windows actuel peut configurer cette option. La barre d'activité d'analyse est disponible uniquement lorsque l'interface est en Mode Expert.

17.2.2. Paramètres du rapport antivirus

- **Envoyer des rapports d'infection** - envoie au laboratoire BitDefender des rapports concernant les virus identifiés sur vote PC. Les informations envoyées contiendront seulement le nom des virus et seront utilisées pour créer des rapports statistiques.

Le rapport ne contiendra aucune donnée confidentielle, comme votre nom, votre adresse IP ou autre et ne sera pas utilisé à des fins commerciales. Les informations envoyées contiendront seulement le nom des virus et seront utilisées pour créer des rapports statistiques.

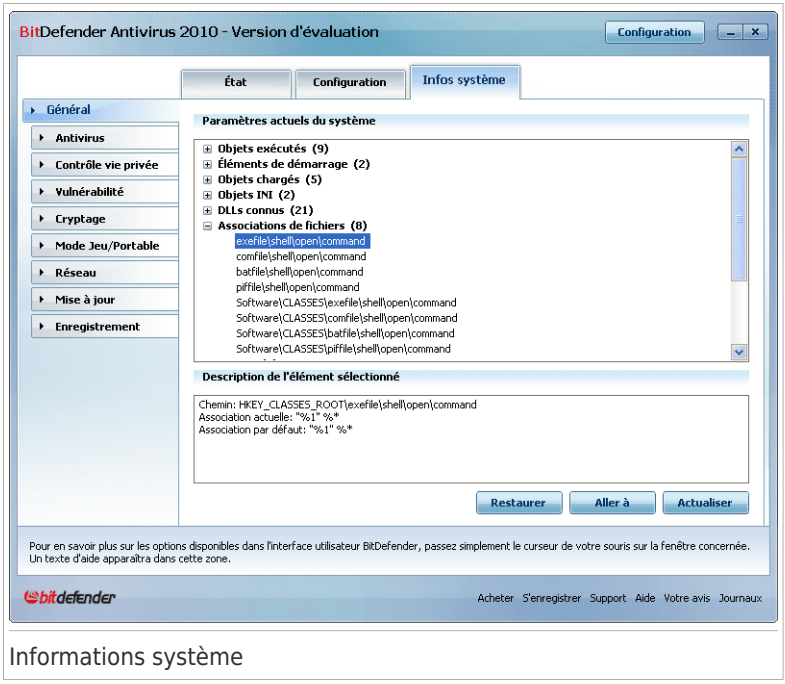
- **Activer l'Outbreak Detection de BitDefender** - envoie des rapports aux BitDefender Labs à propos d'apparitions éventuelles de virus.

  Le rapport ne contiendra aucune donnée confidentielle, comme votre nom, votre adresse IP ou autre et ne sera pas utilisé à des fins commerciales. Les informations envoyées contiendront uniquement les virus potentiels et seront utilisées dans le seul but de créer des rapports statistiques.

17.3. Informations système

BitDefender vous permet d'afficher, à partir d'un emplacement unique, tous les paramètres du système ainsi que les applications enregistrées pour être exécutées au démarrage. Vous pouvez ainsi contrôler l'activité du système et des applications installées et identifier d'éventuelles infections.

Pour obtenir des informations sur le système, allez dans **Général>Infos Système** en Mode Expert.



Informations système

La liste contient tous les objets chargés au démarrage du système ainsi que les objets chargés par différentes applications.

Trois boutons sont disponibles:

- **Restaurer** - modifie une association de fichiers actuelle vers le niveau par défaut. Disponible pour les paramètres d' **associations de fichiers** uniquement !
- **Aller à** - ouvre une fenêtre où l'objet a été placé (la **Base de Registres** par exemple).

Note
Suivant l'objet sélectionné, le bouton **Aller vers** peut ne pas apparaître.

- **Actualiser** - re-ouvre la section **Informations système**.

18. Antivirus

BitDefender protège votre ordinateur contre tous les types de malware (virus, chevaux de Troie, spywares, rootkits, etc.). La protection offerte par BitDefender est divisée en deux catégories:

- Protection en temps réel - empêche les nouvelles menaces d'infecter votre système. BitDefender analysera par exemple un document Word quand vous l'ouvrez, et les e-mails lors de leur réception.

Note

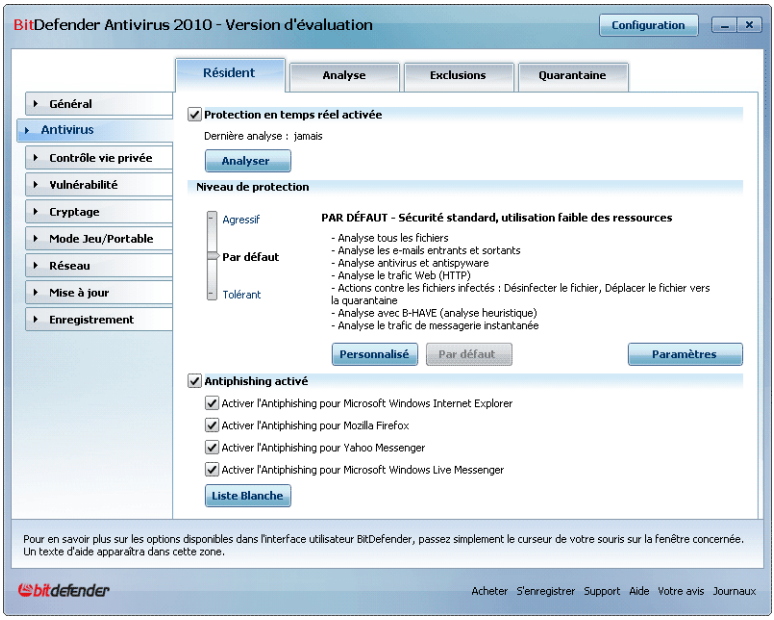
À propos de la protection en temps réel, on parle aussi d'analyse à l'accès – les fichiers sont analysés quand l'utilisateur veut les ouvrir.

- Analyse à la demande - permet de détecter et de supprimer les codes malveillants déjà présents dans le système. C'est l'analyse classique antivirus déclenchée par l'utilisateur – vous choisissez le lecteur, dossier ou fichier que BitDefender doit analyser et BitDefender le fait – A la demande. Les tâches d'analyse permettent de créer des programmes d'analyse personnalisés qui peuvent être planifiés pour être exécutés régulièrement.

18.1. Protection en temps réel

BitDefender protège votre ordinateur de manière continue et en temps réel contre toutes les menaces de codes malveillants en analysant tous les fichiers à l'accès, les e-mails et les communications via les applications de messagerie instantanée (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger). L'antiphishing BitDefender empêche la divulgation de vos informations personnelles sur Internet en vous alertant sur les pages Internet potentiellement de type phishing.

Pour configurer la protection en temps réel et l'Antiphishing BitDefender, allez dans **Antivirus>Résident** en Mode Expert.


BitDefender Antivirus 2010 - Version d'évaluation
Configuration
Résident
Analyse
Exclusions
Quarantaine
Général
Antivirus
Contrôle vie privée
Vulnérabilité
Cryptage
Mode Jeu/Portable
Réseau
Mise à jour
Enregistrement
Protection en temps réel activée
Dernière analyse : jamais
Analyser
Niveau de protection
Agressif
Par défaut
Tolérant
PAR DÉFAUT - Sécurité standard, utilisation faible des ressources
- Analyse tous les fichiers
- Analyse les e-mails entrants et sortants
- Analyse antivirus et antispyware
- Analyse le trafic Web (HTTP)
- Actions contre les fichiers infectés : Désinfecter le fichier, Déplacer le fichier vers la quarantaine
- Analyse avec B-HAVE (analyse heuristique)
- Analyse le trafic de messagerie instantanée
Personnalisé
Par défaut
Paramètres
Antiphishing activé
Activer l'Antiphishing pour Microsoft Windows Internet Explorer
Activer l'Antiphishing pour Mozilla Firefox
Activer l'Antiphishing pour Yahoo Messenger
Activer l'Antiphishing pour Microsoft Windows Live Messenger
Liste Blanche
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

Protection en temps réel

Vous pouvez vérifier si la protection en temps réel est activée ou désactivée. Si vous voulez modifier l'état de la protection en temps réel, cochez ou décochez la case correspondante.

Important
Pour prévenir l'infection de votre ordinateur par des virus, laissez la **protection en temps réel** activée.

Pour lancer une analyse du système, cliquez sur **Analyser**.

18.1.1. Configuration du niveau de protection

Vous pouvez choisir le niveau de protection qui répond le mieux à vos besoins de sécurité. Déplacez le curseur sur l'échelle pour choisir le niveau approprié.

Il existe trois niveaux de protection:

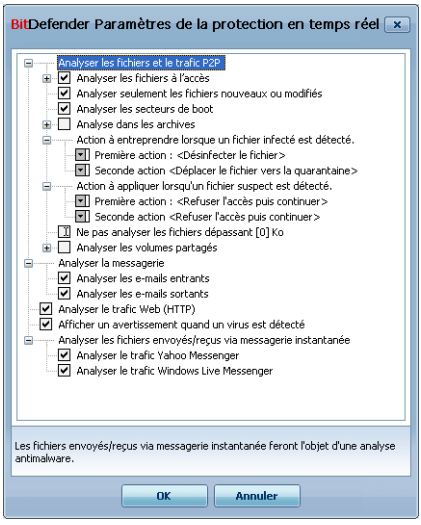
Niveau de protection	Description
Tolérant	Couvre les besoins de sécurité de base. La consommation de ressources système est très faible. Seuls les programmes et les e-mails entrants font l'objet d'une analyse antivirus. Outre l'analyse classique par signatures, l'analyse heuristique est également utilisée. Les actions entreprises contre les fichiers infectés sont les suivantes : désinfecter le fichier / placer le fichier en quarantaine.
Par défaut	Offre un niveau de sécurité standard. La consommation de ressources système est faible. Tous les fichiers et les e-mails entrants et sortants font l'objet d'une analyse antivirus et antispyware. Outre l'analyse classique par signatures, l'analyse heuristique est également utilisée. Les actions entreprises contre les fichiers infectés sont les suivantes : désinfecter le fichier / placer le fichier en quarantaine.
Agressif	Offre un niveau de sécurité élevé. La consommation de ressources système est modérée. Tous les fichiers, les e-mails entrants et sortants ainsi que le trafic Web font l'objet d'une analyse antivirus et antispyware. Outre l'analyse classique par signatures, l'analyse heuristique est également utilisée. Les actions entreprises contre les fichiers infectés sont les suivantes : désinfecter le fichier / placer le fichier en quarantaine.

Pour appliquer les paramètres de protection en temps réel, cliquez sur **Par Défaut**.

18.1.2. Personnaliser le niveau de protection

Les utilisateurs avancés peuvent utiliser les paramètres d'analyse proposés par BitDefender. Le moteur d'analyse peut être configuré pour analyser uniquement des extensions de fichiers spécifiques, pour rechercher des menaces de codes malveillants spécifiques ou pour passer les archives. Cela peut permettre de réduire considérablement la durée d'une analyse et d'améliorer la réactivité de votre ordinateur lors de l'analyse.

Vous pouvez personnaliser la **protection en temps réel** en cliquant sur **Niveau personnalisé**. La fenêtre suivante apparaîtra:



Configuration du résident

Les options d'analyse sont organisées en menus extensibles similaires à ceux utilisés dans l'explorateur Windows. Cliquez la case avec "+" pour ouvrir une option ou la case avec "-" pour fermer une option.

Note

Vous pouvez observer que certaines options d'analyse, bien que le signe "+" apparaisse, ne peuvent s'ouvrir. La raison est que ces options n'ont pas encore été sélectionnées. Vous observerez que si vous les cochez, elles pourront être ouvertes.

- Sélectionner **Analyser à l'accès les fichiers et les transferts P2P** - pour analyser les fichiers à l'accès ainsi que les communications et échanges Peer To Peer (messageries instantanées comme ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger – logiciels de téléchargement comme Kazaa, Emule, Shareaza). Après cela, sélectionnez le type de fichiers que vous voulez analyser.

Option		Description
Analyser les fichiers accédés	**Analyse de tous les fichiers**	Tous les fichiers seront analysés à l'accès, quel que soit leur type.
	Analyser uniquement les extensions d'applications	Seuls les fichiers avec les extensions suivantes seront analysés : `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`;

Option		Description
		.ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml et .nws.
	Analyse les extensions définies par l'utilisateur	Seuls les fichiers avec les extensions définies par l'utilisateur seront analysés. Ces extensions doivent être séparées par ";".
	Rechercher des riskware	Analyses contre les risques non-viraux Les fichiers détectés sont traités en tant que fichiers infectés. Un logiciel incluant des composants de type adware peut ne plus fonctionner si cette option est activée. Sélectionnez **Ne pas analyser les dialers et les applications** et/ou **Ne pas analyser les keyloggers** si vous souhaitez exclure ce type de fichiers de l'analyse.
Analyser uniquement les fichiers nouveaux et modifiés		Analyse uniquement les fichiers qui n'ont pas été analysés auparavant ou qui ont été modifiés depuis la dernière analyse. En sélectionnant cette option, vous pouvez améliorer considérablement la réactivité globale du système avec un minimum de compromis en matière de sécurité.
Analyser les secteurs de boot		Pour analyser les secteurs de boot du système.
Analyser dans les archives		Les archives serons également analysées. Avec cette option activée, l'ordinateur sera ralentit. Vous pouvez définir la taille maximale des archives à analyser (en kilo-octets, tapez 0 si vous souhaitez que toutes les archives soient analysées) et la profondeur maximale des archives à analyser.
Première action		Sélectionnez à partir du menu déroulant la première action à entreprendre sur les fichiers suspicieux et infectés.

Option		Description
	Interdire l'accès et continuer	Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.
	Désinfecter le fichier	Supprime le code malveillant des fichiers infectés.
	Effacer le fichier	Supprime immédiatement les fichiers infectés, sans avertissement.
	Déplacer en quarantaine	Déplace les fichiers infectés dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.
Deuxième action		Sélectionnez à partir du menu déroulant la deuxième action à appliquer sur les fichiers infectés, au cas où la première action échoue.
	Interdire l'accès et continuer	Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.
	Effacer le fichier	Supprime immédiatement les fichiers infectés, sans avertissement.
	Déplacer en quarantaine	Déplace les fichiers infectés dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.
Ne pas analyser les fichiers dont la taille est supérieure à [x] Ko		Tapez la taille maximum des fichiers à analyser. Si vous mettez la taille à 0, tous les fichiers seront analysés.
Analyser les volumes partagés	**Analyse de tous les fichiers**	Tous les fichiers accédés à partir du réseau seront analysés, quel que soit leur type.
	Analyser uniquement les extensions d'applications	Seuls les fichiers avec les extensions suivantes seront analysés : `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml` et `.nws`.

Option		Description
	Analyse les extensions définies par l'utilisateur	Seuls les fichiers avec les extensions définies par l'utilisateur seront analysés. Ces extensions doivent être séparées par ";".

- **Analyser le trafic de messagerie** - analyse le trafic de la messagerie.

  Voici les options proposées :

Option	Description
Analyser les e-mails entrants	Analyser tous les emails entrants.
Analyser les emails sortants	Analyser tous les emails sortants.

- **Analyser le trafic Web (HTTP)** - analyse le trafic http.
- **Afficher une alerte si un virus est trouvé** - une fenêtre d'alerte sera affichée lors de la rencontre d'un virus dans un fichier ou message e-mail.

  Pour un fichier infecté, la fenêtre d'alerte va contenir le nom du virus, le chemin, l'action effectuée par BitDefender et un lien vers le site BitDefender où on peut trouver plus d'informations sur celui-ci. Pour un message e-mail infecté, la fenêtre d'alerte va contenir aussi l'information sur l'expéditeur et le destinataire.

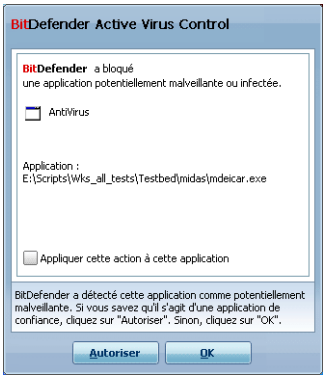
  Au cas où un fichier suspect est détecté vous pouvez lancer un assistant à partir de la fenêtre d'alerte qui vous aidera envoyer ce fichier au Laboratoire BitDefender pour une analyse ultérieure. Vous pouvez saisir votre adresse email pour recevoir des informations sur ce rapport.
- **Analyser les fichiers reçus/envoyés par la messagerie instantanée.** Pour analyser les fichiers que vous recevez ou envoyez via Yahoo ou Windows Live Messenger, cochez la case correspondante.

Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

18.1.3. Configuration d'Active Virus Control

La technologie Active Virus Control (AVC) de BitDefender est un niveau de protection supplémentaire contre les nouvelles menaces pour lesquelles aucune signature n'est encore disponible. Elle surveille et analyse en permanence le comportement des applications qui s'exécutent sur votre ordinateur et vous prévient en cas de comportement suspicieux.

Active Virus Control peut être configuré pour vous prévenir et vous demander d'entreprendre une action lorsqu'une application essaie de réaliser une action potentiellement malveillante.


BitDefender Active Virus Control
BitDefender a bloqué
une application potentiellement malveillante ou infectée.
AntiVirus
Application :
E:\Scripts\Wks_all_tests\Testbed\midas\mdeicar.exe
Appliquer cette action à cette application
BitDefender a détecté cette application comme potentiellement malveillante. Si vous savez qu'il s'agit d'une application de confiance, cliquez sur "Autoriser". Sinon, cliquez sur "OK".
Autoriser
OK

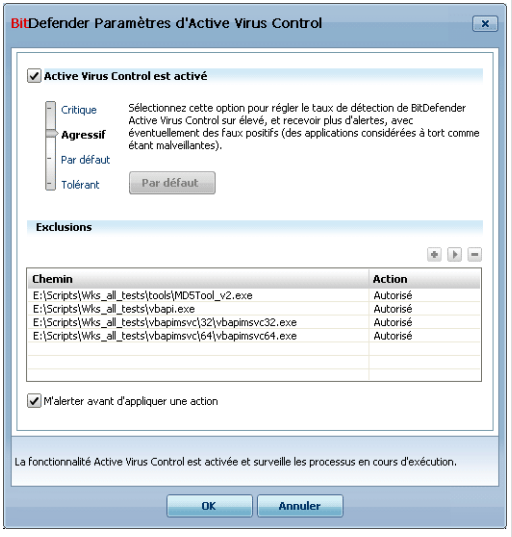
Alerte Active Virus Control

Si vous connaissez l'application et la savez de confiance, cliquez sur **Autoriser**.

Si vous voulez fermer immédiatement cette application, cliquez sur **OK**.

Cochez la case **Retenir cette action pour cette application** avant de faire votre choix et BitDefender réalisera la même action pour l'application détectée par la suite. La règle ainsi créée apparaîtra dans la fenêtre de configuration d'Active Virus Control.

Pour configurer Active Virus Control, cliquez sur **Paramètres Avancés**.



Configuration d'Active Virus Control

Cochez la case correspondante pour activer Active Virus Control.

Important
Conservez Active Virus Control activé pour être protégé(e) contre les virus inconnus.

Si vous souhaitez qu'Active Virus Control vous prévienne et vous demande quelle action entreprendre lorsqu'une application essaie de réaliser une action potentiellement malveillante, cochez la case **Me consulter avant d'entreprendre une action**.

Configuration du niveau de protection

Le niveau de protection d'Active Virus Control change automatiquement lorsque vous modifiez le niveau de protection en temps réel. Si vous n'êtes pas satisfait des paramètres par défaut, vous pouvez configurer manuellement le niveau de protection.

Note

Gardez à l'esprit que si vous modifiez le niveau de protection en temps réel, le niveau de protection d'Active Virus Control sera également modifié. Si vous réglez la protection en temps réel sur **Tolérant**, Active Virus Control est automatiquement désactivé. Dans ce cas, vous pouvez activer manuellement Active Virus Control si vous voulez l'utiliser.

Déplacez le curseur vers le niveau qui correspond le mieux à vos besoins en termes de niveau de protection.

Niveau de protection	Description
Critique	Surveillance stricte de toutes les applications à la recherche d'actions malveillantes.
Par défaut	Les taux de détection sont élevés et les faux positifs sont possibles.
Moyen	La surveillance des applications est modérée, des faux positifs sont possibles.
Tolérant	Les taux de détection sont faibles et il n'y a pas de faux positifs.

Gestion de la liste des Applications de confiance / non fiables

Vous pouvez ajouter à la Liste des applications de confiance des applications que vous connaissez et en lesquelles vous avez confiance. Ces applications ne seront plus contrôlées par BitDefender Active Virus Control et seront automatiquement autorisées.

Les applications pour lesquelles des règles ont été créées apparaissent dans le tableau **Exclusions**. Le chemin vers l'application et l'action que vous avez définie pour celle-ci (Autorisée ou Bloquée) sont indiqués pour chaque règle.

Pour modifier l'action pour une application, cliquez sur l'action actuelle et sélectionnez l'autre action à partir du menu.

Pour gérer la liste, utilisez les boutons placés au-dessus du tableau :

- **Ajouter** - ajoute une nouvelle application à la liste.
- **Supprimer** - supprime une application de la liste.
- **Éditer** - permet de modifier une règle d'application.

18.1.4. Désactivation de la protection en temps réel

Si vous tentez de désactiver la protection en temps réel, une fenêtre d'avertissement apparaît. Vous devez confirmer votre choix en sélectionnant dans le menu la durée pendant laquelle vous souhaitez désactiver la protection en temps réel. Vous pouvez désactiver la protection en temps réel pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.

Avertissement

Cela peut poser un problème de sécurité important. Nous vous recommandons de désactiver la protection en temps réel pendant le moins de temps possible. Si la protection en temps réel est désactivée, vous ne serez pas protégé contre les menaces de codes malveillants.

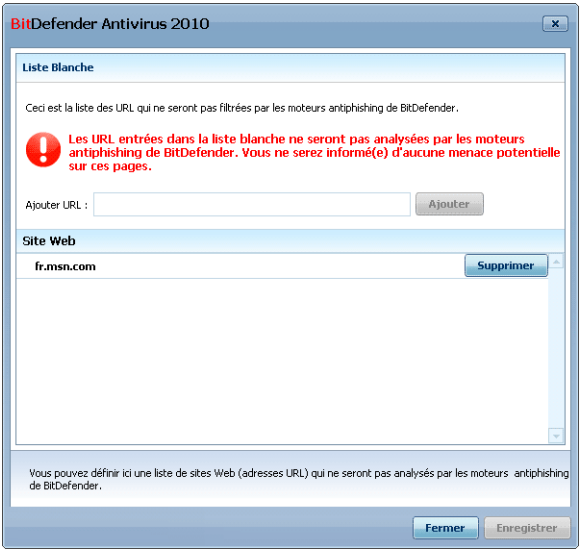
18.1.5. Configurer la protection antiphishing

BitDefender fournit une protection antiphishing en temps réel pour :

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Vous pouvez désactiver la protection antiphishing entièrement ou pour des applications spécifiques uniquement.

Cliquez sur **Liste blanche** pour configurer et gérer une liste de sites Internet à ne pas être analysée par les moteurs antiphishing BitDefender.


BitDefender Antivirus 2010
Liste Blanche
Ceci est la liste des URL qui ne seront pas filtrées par les moteurs antiphishing de BitDefender.
Les URL entrées dans la liste blanche ne seront pas analysées par les moteurs antiphishing de BitDefender. Vous ne serez informé(e) d'aucune menace potentielle sur ces pages.
Ajouter URL :
Ajouter
Site Web
fr.msn.com
Supprimer
Vous pouvez définir ici une liste de sites Web (adresses URL) qui ne seront pas analysés par les moteurs antiphishing de BitDefender.
Fermer
Enregistrer

Liste blanche antiphishing

Vous pouvez visualiser la liste de tous les sites Internet qui ne seront pas analysés par les moteurs antiphishing BitDefender.

Pour ajouter un site Internet à la liste blanche, entrez son adresse url dans le champ **Nouvelle adresse** et cliquez sur **Ajouter**. La Liste Blanche ne doit contenir que des sites web de confiance. Par exemple, ajoutez les sites Web sur lesquels vous avez l'habitude de faire vos achats en ligne.

Note

Vous pouvez ajouter de nouveaux sites Internet à la liste blanche très simplement à partir de la barre d'outils antiphishing de BitDefender intégrée à votre navigateur Internet. Pour plus d'informations, reportez-vous à « *Intégration dans les navigateurs Internet* » (p. 207).

Si vous voulez effacer un site Internet de la liste blanche, cliquez sur le bouton **Effacer**.

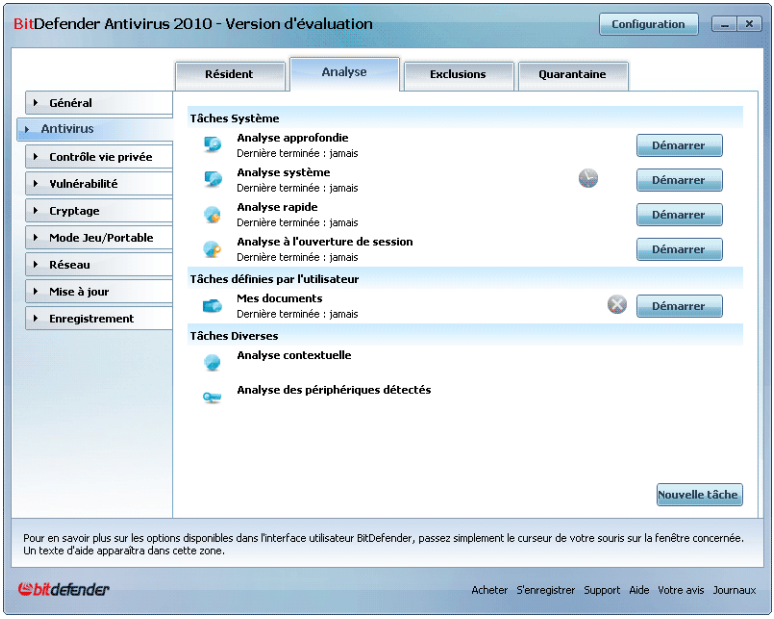
Cliquez sur **Enregistrer** pour sauvegarder les modifications et fermer la fenêtre.

18.2. Analyse à la demande

L'objectif principal de BitDefender est de conserver votre PC sans virus. Cela est assuré avant tout par l'analyse antivirus des emails que vous recevez et des fichiers que vous téléchargez ou copiez sur votre système.

Il y a cependant un risque qu'un virus soit déjà logé dans votre système, avant même l'installation de BitDefender. C'est pourquoi il est prudent d'analyser votre ordinateur après l'installation de BitDefender. Et c'est encore plus prudent d'analyser régulièrement votre ordinateur contre les virus.

Pour configurer et lancer une analyse à la demande, cliquez sur **Antivirus> Analyse** en Mode Expert.



Tâches d'analyse

L'analyse sur demande est basée sur les tâches d'analyse. Les tâches d'analyse permettent de spécifier les options d'analyse et les objets à analyser. Vous pouvez analyser votre ordinateur à tout moment en exécutant les tâches par défaut ou vos propres tâches d'analyse (tâches définies par l'utilisateur). Vous pouvez aussi les planifier pour être exécutées régulièrement ou lorsque votre système est inactif afin de ne pas interférer dans votre travail.

18.2.1. Tâches d'analyse

BitDefender comporte plusieurs tâches créées par défaut qui permettent de traiter les problèmes de sécurité les plus courants. Vous pouvez aussi créer vos propres tâches d'analyse personnalisées.

Il y a trois catégories de tâches d'analyse:

- **Tâches système** - contiennent une liste des tâches système par défaut. Les tâches suivantes sont disponibles:

Tâche d'analyse par défaut	Description
Analyse approfondie du système	Analyse l'ensemble du système. La configuration par défaut permet d'analyser tous les types de codes malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse du Système	Analyse l'ensemble du système, mis à part les archives. Dans la configuration par défaut, l'analyse recherche tous les types de malwares à l'exception des rootkits.
Analyse rapide du système	Analyse les dossiers `Windows` et `Program Files` La configuration par défaut permet d'analyser tous les types de codes malveillants, à l'exception des rootkits, mais ne permet pas d'analyser la mémoire, les registres et les cookies.
Analyse automatique à l'ouverture de session	Analyse les éléments qui sont exécutés quand un utilisateur se connecte à Windows. Par défaut, l'analyse à l'ouverture de session est désactivée. Si vous voulez utiliser cette tâche, faites un clic-droit dessus, sélectionnez **Planifier** et définissez la tâche à exécuter **au démarrage du système**. Spécifiez combien de temps après le démarrage la tâche doit s'exécuter (en minutes).

Note

Sachant que les tâches d'**Analyse approfondie du système** et **d'Analyse complète du système** analysent l'intégralité du système, l'analyse peut prendre un certain temps. C'est pourquoi nous vous recommandons d'exécuter ces tâches en priorité faible ou, si cela est possible, lorsque votre système est inactif.

- **Tâches prédéfinies** - contiennent les tâches prédéfinies par l'utilisateur.

Une tâche Mes documents vous est proposée. Utilisez-la pour analyser les dossiers importants de l'utilisateur actuel: Mes documents, Bureau et Démarrage. Cela vous permet d'assurer la sécurité de vos documents, un espace de travail sécurisé et d'exécuter des applications saines au démarrage.

- **Tâches diverses** - contiennent une liste de tâches diverses. Ces tâches font réference à des modes d'analyse différents qui ne peuvent pas être lancés depuis cette fenêtre. Vous pouvez uniquement modifier leurs paramètres et voir le rapport d'analyse.

Chaque tâche a une fenêtre **Propriétés** qui vous permet de la configurer et d'afficher les journaux d'analyse. Pour ouvrir cette fenêtre, double-cliquez sur la tâche ou cliquez sur le bouton **Propriétés** qui se trouve devant le nom de la tâche. Pour plus d'informations, reportez-vous à « *Configuration des tâches d'analyse* » (p. 121).

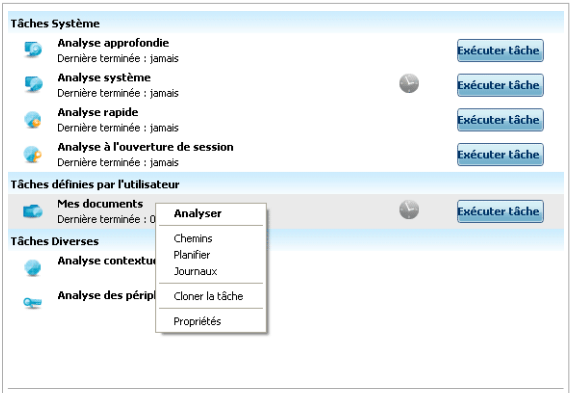
Pour exécuter une tâche d'analyse système ou définie par un utilisateur, cliquez sur le bouton correspondant **Exécuter Tâche**. L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse.

Lorsqu'une tâche est planifiée pour s'exécuter automatiquement, plus tard ou régulièrement, le bouton **Planification** apparaît à droite de la tâche. Cliquez sur ce bouton pour ouvrir la fenêtre **Propriétés**, sur l'onglet Planificateur, où vous pouvez voir la planification de tâche et la modifier.

Si vous n'avez plus besoin d'une tâche d'analyse que vous avez créée (une tâche définie par l'utilisateur), vous pouvez la supprimer en cliquant sur le bouton **Supprimer**, situé à droite de la tâche. Vous ne pouvez pas supprimer les tâches système ou diverses.

18.2.2. Utilisation du menu de raccourcis

Un menu de raccourcis est également disponible pour chaque tâche. Utilisez le "clic-droit" sur la tâche seléctionnée pour y accéder.



Menu de raccourcis

Pour les tâches système et définies par l'utilisateur, les commandes suivantes sont disponibles dans le menu de raccourcis :

- **Analyser** - démarre immédiatement la tâche d'analyse choisie.
- **Chemins** - ouvre la fenêtre **Propriétés** et l'onglet Chemins permettant de modifier la cible à analyser de la tâche sélectionnée.

  Note
  Dans le cas de tâches système, cette option est remplacée par **Montrer les chemins de l'analyse**, car vous ne pouvez voir que leur cible d'analyse.

- **Planifier** - ouvre la fenêtre **Propriétés** et l'onglet Planificateur permettant de planifier la tâche sélectionnée.
- **Afficher les journaux** - ouvre la fenêtre **Propriétés** , et l'onglet Journaux, où vous pouvez voir les rapports générés après l'exécution de la tâche sélectionnée.
- **Cloner la tâche** - reproduit la tâche sélectionnée. Très utile lors de la création de nouvelles tâches car cette fonction vous permet aussi d'en modifier les propriétés si besoin.
- **Effacer** - efface la tâche sélectionnée.

  Note
  Option non disponible pour les tâches d'analyse du système. Vous ne pouvez pas supprimer une tâche d'analyse du système.

- **Propriétés** - ouvre la fenêtre **Propriétés** et l'onglet Résumé permettant de modifier les paramètres de la tâche sélectionnée.

Seules les options des onglets **Propriétés** et **Afficher les journaux** sont disponibles dans la catégorie **Tâches diverses**.

18.2.3. Création de tâches d'analyse

Pour créer une tâche d'analyse, utilisez l'une des méthodes suivantes :

- Clonez une tâche existante, renommez-la et effectuez les modifications nécessaires dans la fenêtre Propriétés.
- **Nouvelle tâche**: permet de créer une nouvelle tâche et de la configurer.

18.2.4. Configuration des tâches d'analyse

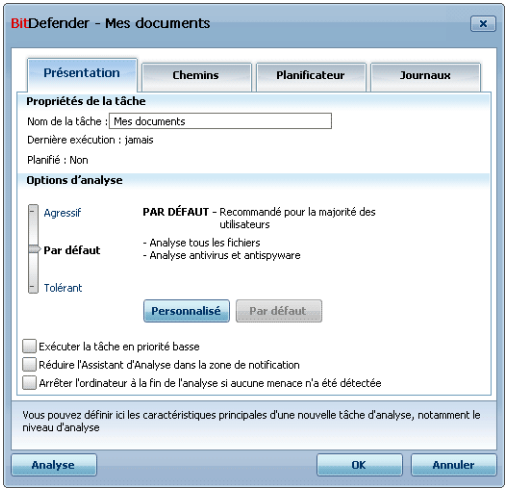
Chaque tâche d'analyse dispose de sa propre fenêtre de **Propriétés**, dans laquelle vous pouvez configurer les options d'analyse, définir les éléments à analyser, programmer une tâche ou voir le rapport. Pour ouvrir cette fenêtre cliquez sur le bouton **Propriétés** à gauche de la tâche (ou faites un clic droit sur la tâche puis cliquez sur **Propriétés**). Vous pouvez aussi double-cliquer sur la tâche.

Note

Pour plus d'informations sur l'affichage des journaux et sur l'onglet **Afficher les journaux**, reportez-vous à « *Afficher les journaux d'analyse* » (p. 141).

Configuration des paramètres d'analyse

Pour configurer les options d'analyse d'une tâche d'analyse spécifique, faites un clic droit dessus et sélectionnez **Propriétés**. La fenêtre suivante apparaît:


BitDefender - Mes documents
Présentation
Chemins
Planificateur
Journaux
Propriétés de la tâche
Nom de la tâche : Mes documents
Dernière exécution : jamais
Planifié : Non
Options d'analyse
Agressif
Par défaut
Tolérant
PAR DÉFAUT - Recommandé pour la majorité des utilisateurs
- Analyse tous les fichiers
- Analyse antivirus et antispyware
Personnalisé
Par défaut
Exécuter la tâche en priorité basse
Réduire l'Assistant d'Analyse dans la zone de notification
Arrêter l'ordinateur à la fin de l'analyse si aucune menace n'a été détectée
Vous pouvez définir ici les caractéristiques principales d'une nouvelle tâche d'analyse, notamment le niveau d'analyse
Analyse
OK
Annuler

Présentation

Vous trouverez dans cette rubrique les informations concernant les tâches (nom, dernière analyse, planification) et aurez la possibilité de définir les paramètres d'analyse.

Sélection du niveau d'analyse

Vous pouvez facilement configurer les paramètres d'analyse en sélectionnant le niveau d'analyse. Déplacez le curseur sur l'échelle pour définir le niveau d'analyse approprié.

Il y a 3 niveaux d'analyse:

Niveau de protection	Description
Tolérant	Offre un niveau de détection correct. La consommation de ressources est faible. Seuls les programmes font l'objet d'une analyse antivirus. En plus de la recherche classique par signature, l'analyse heuristique est également utilisée.
Moyen	Offre un niveau de détection efficace. La consommation de ressources système est modérée. Tous les fichiers sont scannés pour détecter les virus et les spywares. En plusde la recherche classique par signature, l'analyse heuristique est également utilisée.
Agressif	Offre un niveau de détection élevé. La consommation de ressources système est élevée. Tous les fichiers et les fichiers archives sont scannés pour détecter les virus et les spywares. En plus de la recherche classique par signature, l'analyse heuristique est également utilisée.

Une série d'options générales de paramétrage de l'analyse sont également disponibles:

- **Exécuter la tâche d'analyse avec une priorité basse.** Décroît la priorité du processus d'analyse. Vous allez permettre aux autres logiciels d'être exécutés à une vitesse supérieure et d'augmenter le temps nécessaire pour le final du processus d'analyse.
- **Réduire l'assistant d'analyse dans la zone de notification.** Réduit la fenêtre d'analyse dans la barre d'état système. Double-cliquez sur l'icône de BitDefender pour l'ouvrir.

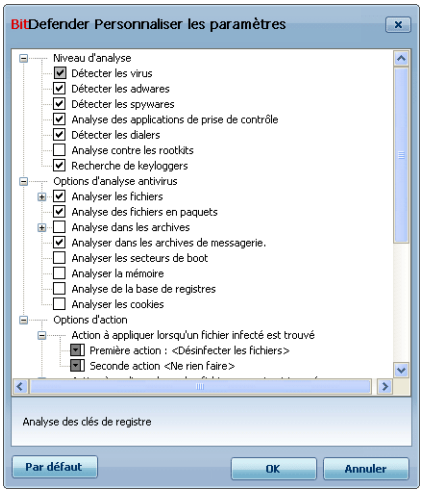
- **Arrêter l'ordinateur lorsque l'analyse est terminée si aucune menace n'a été détecté**

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

Personnalisation du niveau d'analyse

Les utilisateurs avancés peuvent utiliser les paramètres d'analyse proposés par BitDefender. Le moteur d'analyse peut être configuré pour analyser uniquement des extensions de fichiers spécifiques, pour rechercher des menaces de codes malveillants spécifiques ou pour passer les archives. Cela peut permettre de réduire considérablement la durée d'une analyse et d'améliorer la réactivité de votre ordinateur lors de l'analyse.

Cliquez sur **Personnalisé** pour définir vos propres options d'analyse. Une nouvelle fenêtre est alors affichée.



Options d'analyse

Les options d'analyse sont organisées en menus extensibles similaires à ceux utilisés dans l'explorateur Windows. Cliquez la case avec "+" pour ouvrir une option ou la case avec "-" pour fermer une option.

Les options d'analyse sont regroupées en trois catégories:

- **Niveau d'analyse.** Spécifiez le type de codes malveillants que vous souhaitez que BitDefender analyse en sélectionnant les options correspondantes dans la catégorie **Niveau d'analyse**.

Option	Description
Analyse antivirus	Analyse les virus connus. BitDefender détecte également les corps de virus incomplets, permettant ainsi d'écarter toute menace potentielle pouvant affecter la sécurité de votre système.
Détecter les adwares	Analyse les menaces d'adwares. Les fichiers détectés sont traités en tant que fichiers infectés. Un logiciel incluant des composants de type adware peut ne plus fonctionner si cette option est activée.
Rechercher les spywares	Analyse les menaces de spywares connus. Les fichiers détectés sont traités en tant que fichiers infectés.
Analyse des applications	Analyser les applications légitimes qui pourraient être utilisées pour cacher des outils d'espionnage ou d'autres applications malicieuses.
Détecter les numéroteurs	Analyse les applications qui appellent des numéros surtaxés. Les fichiers détectés sont traités en tant que fichiers infectés. Un logiciel incluant des composants de type numéroteur peut ne plus fonctionner si cette option est activée.
Analyse des rootkits	Analyse les objets cachés (fichiers et processus), plus connus sous le nom de rootkits.

- **Options d'analyse antivirus.** Spécifiez le type d'objets à analyser (types de fichiers, archives, etc.) en sélectionnant les options appropriées dans la catégorie **Options d'analyse antivirus**.

Option		Description
Analyser les fichiers	**Analyse de tous les fichiers**	Tous les fichiers seront analysés, quel que soit leur type.
	Analyse des extensions à risques seulement	Seuls les fichiers avec les extensions suivantes seront analysés: `exe`; `bat`; `com`; `dll`; `ocx`; `scr`; `bin`; `dat`; `386`; `vxd`; `sys`; `wdm`; `cla`; `class`; `ovl`; `ole`; `exe`; `hlp`; `doc`; `dot`; `xls`; `ppt`; `wbk`; `wiz`; `pot`; `ppa`; `xla`; `xlt`; `vbs`; `vbe`; `mdb`; `rtf`; `htm`; `hta`; `html`; `xml`; `xtp`; `php`; `asp`; `js`; `shs`; `chm`; `lnk`; `pif`;

Option		Description
		prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml et nws.
	Analyse les extensions définies par l'utilisateur	Seuls les fichiers avec les extensions définies par l'utilisateur seront analysés. Ces extensions doivent être séparées par ";".
Analyser dans les fichiers en paquets		Analyser les fichiers en paquets.
Analyser dans les archives		Analyse les archives standards, comme .zip, .rar, .ace, .iso et les autres. Cochez la case **Analyser les programmes d'installation et les archives chm** si vous souhaitez que ces types de fichiers soient analysés. L'analyse des fichiers archive augmente le temps d'analyse et demande plus de ressource système. Vous pouvez définir la taille maximale des archives à analyser en kilo-octets (Ko) en tapant la taille dans le champ **Limiter la taille des archives analysées à**.
Analyser dans les archives de messagerie		Analyser dans les archives de messagerie.
Analyser les secteurs de boot		Pour analyser les secteurs de boot du système.
Analyse de la mémoire		Analyser la mémoire pour détecter les virus et les autres malwares.
Analyse la base de registre		Analyse les entrées du Régistre.
Analyse les cookies		Analyse les cookies.

- **Options d'action.** Spécifiez les actions à appliquer pour chaque catégorie de fichiers détectés en utilisant les options de cette catégorie.

Note

Pour définir une nouvelle action, cliquez sur **Première action** et sélectionnez l'option souhaitée dans le menu. Indiquez une **Seconde action** qui sera appliquée si la première échoue.

▶ Sélectionnez l'action à mener sur les fichiers infectés détectés. Voici les options proposées :

Action	Description
Ne pas mener d'action	Aucune action ne sera prise sur les fichiers infectés. Ceux-ci vont apparaître dans le fichier des rapports.
Désinfecter	Supprimer le code malveillant des fichiers infectés.
Supprimer les fichiers	Supprime immédiatement les fichiers infectés, sans avertissement.
Déplacer vers la quarantaine	Déplace les fichiers infectés dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.

▶ Sélectionnez l'action à mener sur les fichiers suspects détectés. Voici les options proposées :

Action	Description
Ne pas mener d'action	Aucune mesure ne sera prise à l'encontre des fichiers suspects. Ces fichiers apparaîtront dans le fichier rapport.
Supprimer les fichiers	Supprime immédiatement les fichiers suspects, sans avertissement.
Déplacer vers la quarantaine	Déplace les fichiers suspects dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.

Note

Les fichiers sont détectés en tant que fichiers suspects par l'analyse heuristique. Nous vous recommandons de les envoyer au laboratoire BitDefender.

▶ Sélectionnez l'action à mener sur les objets cachés (rootkits) détectés. Voici les options proposées :

Action	Description
Ne pas mener d'action	Aucune mesure ne sera prise à l'encontre des fichiers cachés. Ces fichiers apparaîtront dans le fichier rapport.
Renommer	Modifie le nom des fichiers cachés en y ajoutant le suffixe `.bd.ren`. Vous pourrez ainsi rechercher ce type de fichiers sur votre ordinateur, et les trouver s'il en existe.
Déplacer vers la quarantaine	Déplace les fichiers cachés dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.

Note

Veuillez noter que ces fichiers cachés ne sont pas ceux que vous avez choisi de ne pas afficher dans Windows. Ce sont des fichiers qui ont été cachés par des programmes particuliers, connus sous le nom de rootkits. Les rootkits ne sont pas malveillants en eux-mêmes. Ils sont cependant couramment utilisés pour rendre les virus et les spywares indétectables par les programmes antivirus habituels.

- **Options d'actions pour les fichiers protégés par un mot de passe et les fichiers cryptés.** Les fichiers cryptés avec Windows peuvent avoir de l'importance pour vous. Cette pour cette raison que vous pouvez configurer différentes mesures à prendre contre les fichiers infectés ou suspects cryptés par Windows. Une autre catégorie de fichiers qui réclament des mesures particulières est celle des archives protégées par mot de passe. Les archives protégées par mot de passe ne peuvent pas être analysées à moins que vous ne communiquiez le mot de passe. Utilisez ces options pour configurer les mesures à prendre vis-à-vis des fichiers d'archives protégées par mot de passe et des fichiers cryptés par Windows.

  - **Action à entreprendre lorsqu'un fichier crypté infecté est détecté.** Sélectionnez la mesure à prendre contre les fichiers infectés cryptés par Windows. Voici les options proposées :

Action	Description
Ne pas entreprendre d'action	N'enregistrer dans le journal que les fichiers infectés cryptés par Windows. Une fois l'analyse terminée, vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.

Action	Description
Désinfecter	Supprimer le code malveillant des fichiers infectés. La désinfection peut échouer dans certains cas, par exemple quand le fichier infecté se trouve dans une archive courrier spécifique.
Supprimer les fichiers	Supprime immédiatement les fichiers infectés, sans avertissement.
Déplacer vers la quarantaine	Déplacer les fichiers infectés de leur emplacement d'origine vers le dossier de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.

- **Action à entreprendre lorsqu'un fichier crypté suspect est détecté.** Sélectionnez la mesure à prendre contre les fichiers suspects cryptés par Windows. Voici les options proposées :

Action	Description
Ne pas entreprendre d'action	N'enregistrer dans le journal que les fichiers suspects cryptés par Windows. Une fois l'analyse terminée, vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.
Supprimer les fichiers	Supprime immédiatement les fichiers suspects, sans avertissement.
Déplacer vers la quarantaine	Déplace les fichiers suspects dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.

- **Action à entreprendre pour les fichiers protégés par mot de passe.** Sélectionnez l'action à entreprendre sur les fichiers protégés par mot de passe détectés. Voici les options proposées :

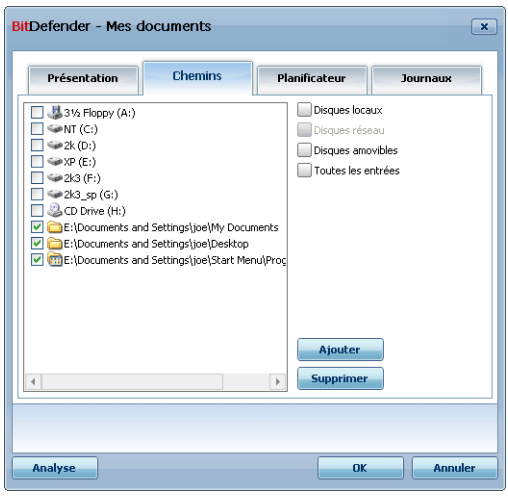
Action	Description
Seulement journaliser	Ne conserver que les enregistrements des fichiers protégés par mot de passe dans le journal d'analyse. Une fois l'analyse terminée,

Action	Description
	vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.
Demander pour le mot de passe	Quand un fichier protégé par mot de passe est détecté, demander à l'utilisateur le mot de passe afin de pouvoir analyser le fichier.

Si vous cliquez sur **Défaut** vous chargerez les paramètres par défaut. Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Définition de la cible à analyser

Pour définir la cible d'une tâche d'analyse d'un utilisateur spécifique, faites un clic droit sur la tâche et sélectionnez **Chemins**. Si vous vous trouvez déjà dans la fenêtre Propriétés d'une tâche, vous pouvez aussi sélectionner l'onglet **Chemins**. La fenêtre suivante apparaît:



Cible de l'Analyse

Vous pouvez afficher la liste des lecteurs locaux, réseau ou amovibles, ainsi que les fichiers ou dossiers ajoutés précédemment, le cas échéant. Tous les éléments cochés seront analysés lors de l'exécution de la tâche.

Voici les différents boutons proposés:

- **Ajouter** - ouvre une fenêtre de navigation vous permettant de sélectionner le(s) fichier(s)/dossier(s) que vous souhaitez analyser.

  Note
  Vous pouvez rajouter des fichiers et des dossiers à la liste d'analyse en les glissant-déposant.

- **Supprimer** - supprime les fichiers/dossiers précédemment sélectionnés de la liste des objets à analyser.

  Note
  Seulement les fichiers/dossiers rajoutés après peuvent être effacés, mais pas ceux qui sont automatiquement "proposés" par BitDefender.

En plus de ces boutons, certaines options permettent une sélection rapide des cibles d'analyse.

- **Disques locaux** - pour analyser les disques locaux.
- **Disques réseaux** - pour analyser tous les lecteurs réseaux.
- **Disques amovibles** - pour analyser les disques amovibles (CD-ROM, lecteur de disquettes).
- **Toutes les entrées** - pour analyser l'ensemble des lecteurs, peu importe qu'ils soient locaux, réseaux ou amovibles.

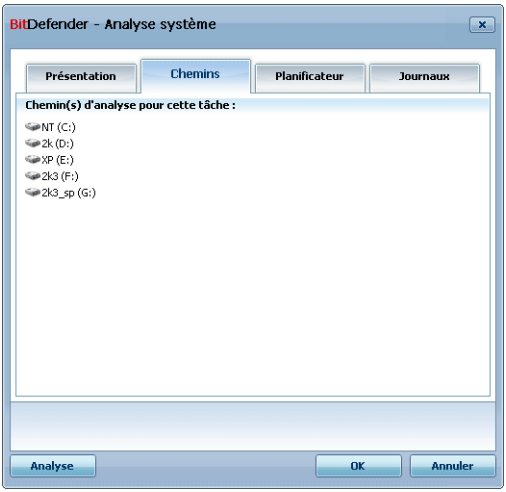
Note
Si vous voulez analyser l'ensemble de votre ordinateur, cochez la case **Toutes les entrées**.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

Voir les cibles d'analyse des tâches système.

Vous ne pouvez pas modifier la cible des tâches d'analyse à partir de la catégorie **Tâches Système**. Vous pouvez seulement visualiser leur cible d'analyse.

Pour voir la cible d'analyse d'une tâche d'analyse système spécifique, faites un clic-droit sur la tâche et sélectionnez **Montrer les chemins de l'analyse**. Pour **Analyse du système**, par exemple, la fenêtre suivante apparaîtra :



Cible de l'Analyse Système

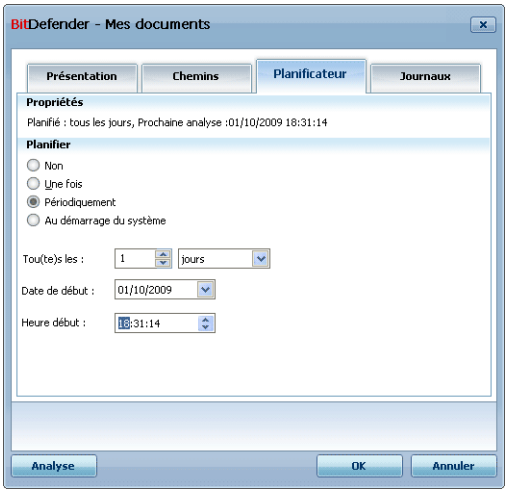
Analyse du Système et **Analyse approfondie du système** analyseront tous les disques locaux, alors que **Analyse rapide du système** analysera uniquement les répertoires `Windows` et `Program Files`.

Cliquez sur **OK** pour fermer la fenêtre. Pour exécuter la tâche, cliquez juste sur **Analyser**.

Planification des tâches d'analyse

Etant donné que l'analyse prendra du temps, et qu'elle fonctionnera mieux si vous avez fermé les autres programmes, il est préférable pour vous de programmer une analyse à une heure où vous n'utilisez pas votre ordinateur. L'utilisateur doit pour cela créer une tâche à l'avance.

Pour voir la planification d'une tâche spécifique ou la modifier, faites un clic droit sur la tâche et sélectionnez **Planifier**. Si vous êtes déjà dans la fenêtre Propriétés d'une tâche, sélectionnez l'onglet **Planificateur**. La fenêtre suivante apparaît:



Planificateur

La tâche planifiée s'affiche, le cas échéant.

Quand vous programmez une tâche, vous devez choisir une des options suivantes :

- **Non** - lance la tâche uniquement à la demande de l'utilisateur.
- **Une fois** - lance l'analyse une fois seulement, à un certain moment. Spécifiez la date et l'heure de démarrage dans le champ **Démarrer Date/Heure**.
- **Périodiquement** - lance une analyse périodiquement, à des intervalles réguliers (minutes, heures, jours, semaines, mois) à compter d'une date et d'une heure spécifiées.

  Si vous voulez que l'analyse se répète à intervalle régulier, cochez la case **Périodiquement** et précisez dans les champs **Toutes/Tous les** le nombre de minutes/heures/jours/semaines/mois. Vous devez également déterminer la date et l'heure de début dans les champs **Date/Heure de début**.
- **Au démarrage système** - démarre l'analyse au moment défini après que l'utilisateur se soit connecté à Windows.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

18.2.5. Analyse des fichiers et des dossiers

Avant de lancer un processus d'analyse, vous devez vous assurer que BitDefender est à jour de ses signatures de codes malveillants. Analyser votre ordinateur en utilisant une base de données de signatures non à jour peut empêcher BitDefender de détecter le nouveau malware identifié depuis la mise à jour précédente. Pour vérifier de quand date la dernière mise à jour, choisissez **Mise à jour>Mise à jour** en Mode avancé.

Note

Afin de permettre à BitDefender de réaliser une analyse complète, il est nécessaire de fermer tous les programmes ouverts, tout spécialement les clients de messagerie (ex : Outlook, Outlook Express ou Eudora).

Astuces d'analyse

Voici quelques astuces supplémentaires qui pourraient vous être utiles :

- Selon la taille de votre disque dur, l'analyse complète de votre ordinateur (Analyse approfondie ou Analyse du système) peut prendre un certain temps (jusqu'à une heure ou même plus). Il est donc préférable de lancer ce type d'analyses à un moment où vous cessez d'avoir besoin de votre ordinateur (au cours de la nuit par exemple).

  Vous pouvez planifier l'analyse pour la faire débuter au moment opportun. Pensez à laisser votre ordinateur allumé. Avec Windows Vista, vérifiez que votre ordinateur ne sera pas en mode veille au moment planifié pour l'exécution de la tâche.

- Si vous téléchargez fréquemment des fichiers sur Internet vers un dossier particulier, créez une nouvelle tâche n'analyse et spécifiez que ce dossier est la cible de l'analyse. Planifiez la tâche pour qu'elle s'exécute quotidiennement ou plus souvent.

- Il existe un type de malware paramétré pour s'exécuter au démarrage du système en modifiant les paramètres de Windows. Pour protéger votre ordinateur contre les malwares de ce type, vous pouvez planifier la tâche **Analyse à l'ouverture de session** pour qu'elle s'exécute au démarrage du système. Veuillez noter que l'analyse à l'ouverture de session peut avoir une influence sur les performances du système pendant un court moment après le démarrage.

Méthodes d'analyse

BitDefender permet quatre types d'analyse à la demande :

- Analyse immediate - lance une tâche d'analyse depuis les tâches disponibles.
- Analyse contextuelle - faites un clic droit sur le fichier ou le dossier et sélectionnez **Analyser avec BitDefender**.
- Analyse par glisser-déposer - glissez & déposez un fichier ou un répertoire sur la barre d'analyse d'activité.

- Analyse manuelle - utilisez l'analyse manuelle BitDefender pour sélectionner directement les fichiers ou répertoires que vous souhaitez analyser.

Analyse immédiate

Vous pouvez analyser tout ou partie de votre ordinateur en exécutant les tâches d'analyse par défaut ou vos propres tâches d'analyse. Cela s'appelle l'analyse immédiate.

Pour exécuter une tâche d'analyse système ou définie par un utilisateur, cliquez sur le bouton correspondant **Exécuter Tâche**. L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse.

Analyse contextuelle

Pour analyser un fichier ou un dossier sans configurer de nouvelle tâche d'analyse, vous pouvez utiliser le menu contextuel. Cela s'appelle l'analyse contextuelle.

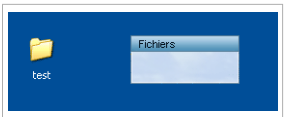
Analyse contextuelle

Faites un clic droit sur le fichier ou le dossier que vous souhaitez analyser et sélectionnez **Analyser avec BitDefender**. L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse.

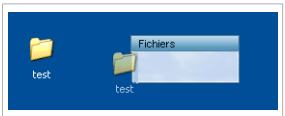
Vous pouvez modifier les options d'analyse et voir les fichiers de rapport à partir de la fenêtre **Propriétés** de la tâche **Analyse via le menu contextuel**.

Analyse par glisser&déposer

Glissez le fichier ou répertoire que vous voulez analyser et déposez-le sur la **Barre d'analyse de l'activité**, comme sur l'image ci-dessous.



Glisser le fichier



Déposer le fichier

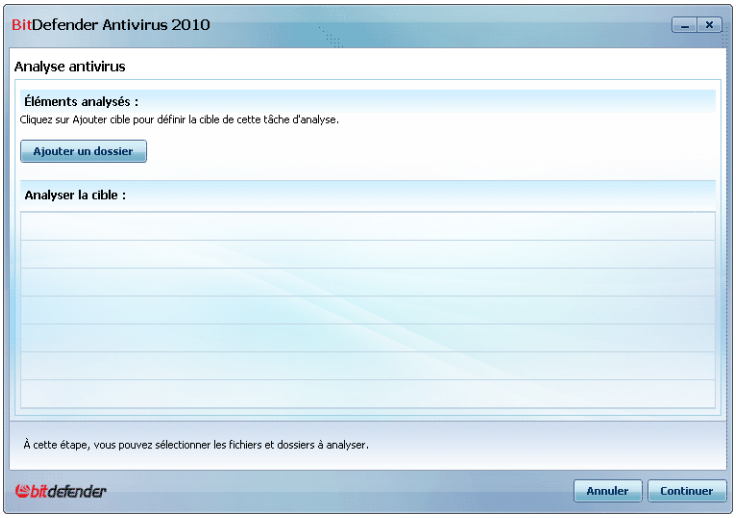
L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse.

Analyse manuelle

L'analyse manuelle consiste à sélectionner directement les fichiers ou répertoires que vous souhaitez analyser avec l'option d'analyse manuelle Bitdefender disponible depuis le menu Démarrer de Windows dans le groupe de programme BitDefender.

Note
L'analyse manuelle est très pratique car elle peut également être effectuée lorsque Windows est en mode sans échec.

Pour sélectionner l'objet que BitDefender doit analyser, suivez ce chemin à partir du menu Démarrer de Windows : **Démarrer → Programmes → BitDefender 2010 → Analyse manuelle BitDefender**. La fenêtre suivante apparaît:


BitDefender Antivirus 2010
Analyse antivirus
Éléments analysés :
Cliquez sur Ajouter cible pour définir la cible de cette tâche d'analyse.
Ajouter un dossier
Analyser la cible :
À cette étape, vous pouvez sélectionner les fichiers et dossiers à analyser.
bitdefender
Annuler
Continuer

Analyse manuelle

Cliquez sur **Ajouter Dossier**, sélectionnez l'emplacement que vous voulez analyser et cliquez sur **OK**. Si vous voulez analyser plusieurs dossiers, répétez cette action pour chaque emplacement supplémentaire.

Les chemins vers les emplacements sélectionnés apparaîtront dans la colonne **Cible de l'Analyse**. Si vous changez d'avis pour un emplacement donné, cliquez simplement sur le bouton **Supprimer** situé en regard de l'emplacement. Cliquez sur le bouton **Supprimer tous les chemins** pour supprimer tous les emplacements qui avaient été ajoutés à la liste.

Une fois les emplacements sélectionnés, cliquez sur **Continuer**. L'Assistant d'analyse antivirus s'affichera et vous guidera au cours du processus d'analyse.

Assistant d'analyse antivirus

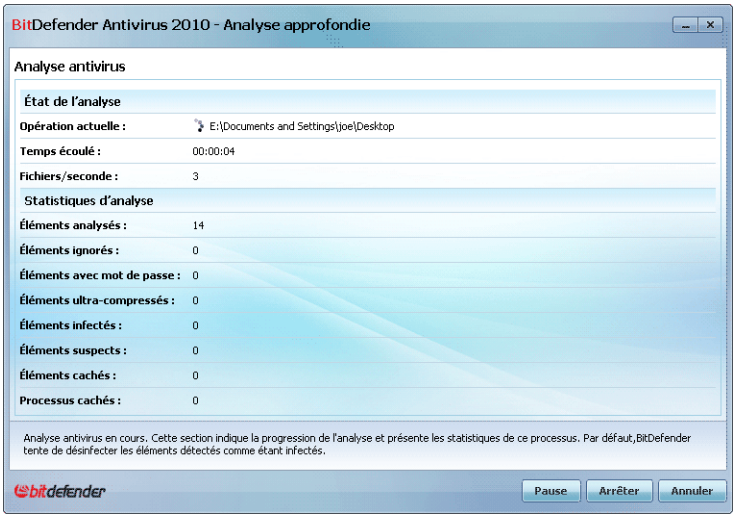
Quand vous lancez une analyse à la demande, l'assistant antivirus s'affiche. Suivez cette procédure en trois étapes pour effectuer le processus d'analyse:

Note

Si l'assistant d'analyse ne s'affiche pas, il est possible que l'analyse soit paramétrée pour s'exécuter invisiblement, en tâche de fond. Recherchez l'icône de l'avancement de l'analyse dans la barre des tâches. Vous pouvez cliquer sur cette icône pour ouvrir la fenêtre d'analyse et suivre son avancement.

Étape 1 sur 3 - Analyse

BitDefender commence à analyser les objets sélectionnés.


BitDefender Antivirus 2010 - Analyse approfondie
Analyse antivirus
État de l'analyse
Opération actuelle : E:\Documents and Settings\joe\Desktop
Temps écoulé : 00:00:04
Fichiers/seconde : 3
Statistiques d'analyse
Éléments analysés : 14
Éléments ignorés : 0
Éléments avec mot de passe : 0
Éléments ultra-compressés : 0
Éléments infectés : 0
Éléments suspects : 0
Éléments cachés : 0
Processus cachés : 0
Analyse antivirus en cours. Cette section indique la progression de l'analyse et présente les statistiques de ce processus. Par défaut,BitDefender tente de désinfecter les éléments détectés comme étant infectés.
bitdefender
Pause
Arrêter
Annuler

Analyse en cours

Le statut et les statistiques de l'analyse s'affichent (vitesse d'analyse, temps écoulé, nombre d'objets analysés / infectés / suspects / cachés, etc.).

Patientez jusqu'à ce que BitDefender ait terminé l'analyse.

Note
L'analyse peut durer un certain temps, suivant sa complexité.

Archives protégées par mot de passe. Si BitDefender détecte pendant l'analyse une archive protégée par mot de passe, et que l'action par défaut est **Demander le mot de passe**, vous serez invité à fournir le mot de passe. Les archives protégées par mot de passe ne peuvent pas être analysées à moins que vous ne communiquiez le mot de passe. Voici les options proposées :

- **Mot de passe.** Si vous souhaitez que BitDefender analyse l'archive, sélectionnez cette option et entrez le mot de passe. Si vous ne connaissez pas le mot de passe, choisissez l'une des autres options.
- **Ne pas demander le mot de passe et ne pas analyser cet objet.** Sélectionnez cette option pour ne pas analyser cette archive.

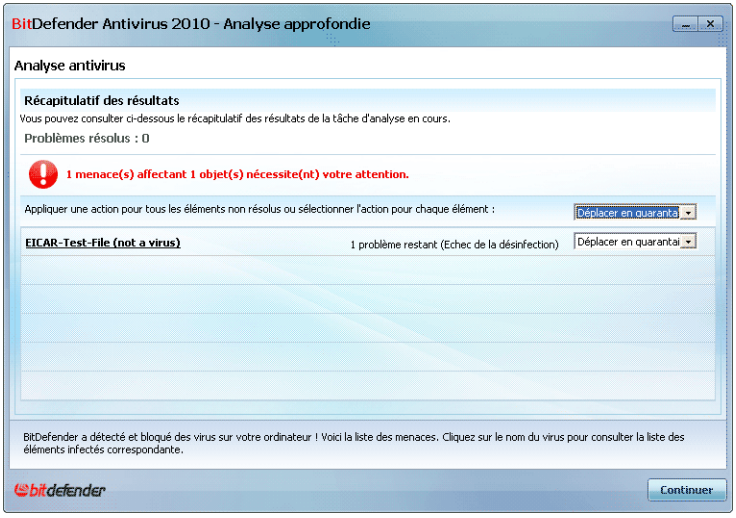
- **Ne pas analyser les éléments protégés par mot de passe.** Sélectionnez cette option si vous ne voulez pas être dérangé au sujet des archives protégées par mot de passe. BitDefender ne pourra pas les analyser, mais un rapport sera conservé dans le journal des analyses.

Cliquez sur **OK** pour continuer l'analyse.

Arrêt ou pause de l'analyse. Vous pouvez arrêter l'analyse à tout moment en cliquant sur **Arrêter et Oui**. Vous vous retrouverez alors à la dernière étape de l'assistant. Pour suspendre temporairement le processus d'analyse, cliquez sur **Pause**. Pour reprendre l'analyse, cliquez sur **Reprendre**.

Étape 2 sur 3 - Sélectionner des actions

Une fois l'analyse terminée, une nouvelle fenêtre apparaît affichant les résultats de l'analyse.


BitDefender Antivirus 2010 - Analyse approfondie
Analyse antivirus
Récapitulatif des résultats
Vous pouvez consulter ci-dessous le récapitulatif des résultats de la tâche d'analyse en cours.
Problèmes résolus : 0
1 menace(s) affectant 1 objet(s) nécessite(nt) votre attention.
Appliquer une action pour tous les éléments non résolus ou sélectionner l'action pour chaque élément :
Déplacer en quarantai
EICAR-Test-File (not a virus)
1 problème restant (Echec de la désinfection)
Déplacer en quarantai
BitDefender a détecté et bloqué des virus sur votre ordinateur ! Voici la liste des menaces. Cliquez sur le nom du virus pour consulter la liste des éléments infectés correspondante.
bitdefender
Continuer

Actions

Le nombre de problèmes de sécurité affectant votre système est indiqué.

Les objets infectés sont affichés dans des groupes, basés sur les malwares les ayant infectés. Cliquez sur le lien correspondant à une menace pour obtenir plus d'informations sur les éléments infectés.

Vous pouvez sélectionner une action globale à mener pour l'ensemble des problèmes de sécurité ou sélectionner des actions spécifiques pour chaque groupe de problèmes.

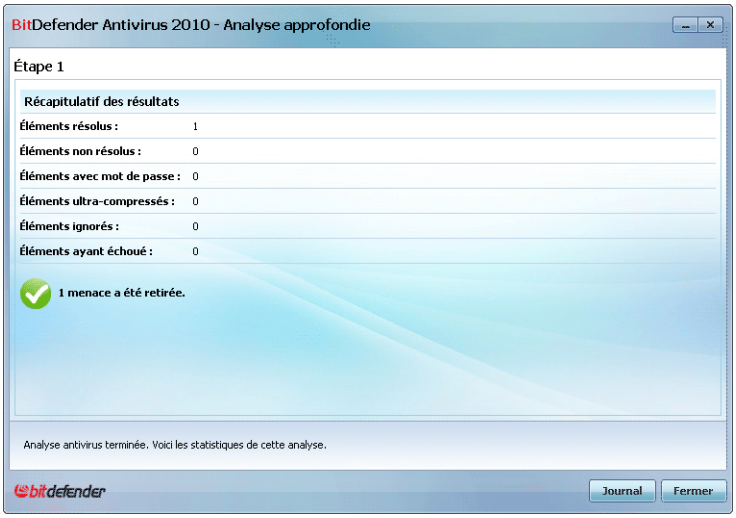
Une ou plusieurs des options qui suivent peuvent apparaître dans le menu :

Action	Description
Ne pas mener d'action	Aucune action ne sera menée sur les fichiers détectés. Une fois l'analyse terminée, vous pouvez ouvrir le journal d'analyse pour visualiser les informations sur ces fichiers.
Désinfecter	Supprime le code malveillant des fichiers infectés.
Supprimer	Supprime les fichiers détectés.
Quarantaine	Déplace les fichiers detectés dans la zone de quarantaine. Les fichiers mis en quarantaine ne peuvent ni être exécutés ni ouverts ; ce qui supprime le risque d'une infection.
Renommer	Modifie le nom des fichiers cachés en y ajoutant le suffixe `.bd.ren`. Vous pourrez ainsi rechercher ce type de fichiers sur votre ordinateur, et les trouver s'il en existe. Veuillez noter que ces fichiers cachés ne sont pas ceux que vous avez choisi de ne pas afficher dans Windows. Ce sont des fichiers qui ont été cachés par des programmes particuliers, connus sous le nom de rootkits. Les rootkits ne sont pas malveillants en eux-mêmes. Ils sont cependant couramment utilisés pour rendre les virus et les spywares indétectables par les programmes antivirus habituels.

Cliquez sur **Continuer** pour appliquer les actions spécifiées.

Étape 3 sur 3 - Voir les résultats

Une fois que les problèmes de sécurité auront été corrigés par BitDefender, les résultats de l'analyse apparaîtront dans une nouvelle fenêtre.


BitDefender Antivirus 2010 - Analyse approfondie
Étape 1
Récapitulatif des résultats
Éléments résolus : 1
Éléments non résolus : 0
Éléments avec mot de passe : 0
Éléments ultra-compressés : 0
Éléments ignorés : 0
Éléments ayant échoué : 0
1 menace a été retirée.
Analyse antivirus terminée. Voici les statistiques de cette analyse.
bitdefender
Journal
Fermer

Récapitulatif

Le récapitulatif des résultats s'affiche. Si vous souhaitez connaître toutes les informations sur le processus d'analyse, cliquez sur **Afficher le journal** pour afficher le journal des analyses.

Important
Si cela est nécessaire, il vous sera demandé de redémarrer votre système pour terminer le processus d'installation.

Cliquez sur **Fermer** pour fermer la fenêtre.

BitDefender n'a pas pu corriger certains problèmes

Dans la plupart des cas, BitDefender désinfecte ou isole l'infection des fichiers infectés qu'il détecte. Cependant, il y a des problèmes qui ne peuvent pas être résolus.

Dans ces cas, nous vous recommandons de contacter le support BitDefender sur le site www.bitdefender.fr. Nos équipes du support technique vous aideront à résoudre les problèmes que vous rencontrez.

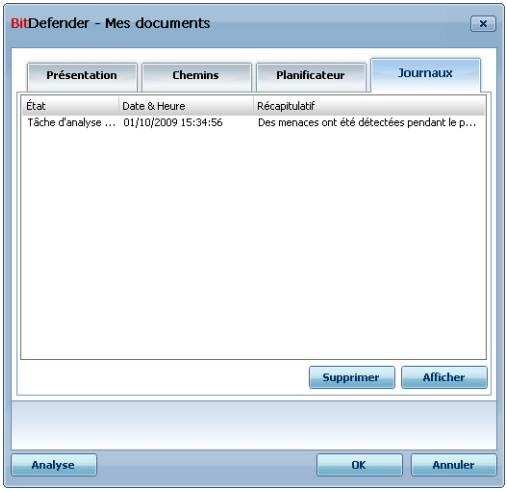
BitDefender a détecté des fichiers suspects

Les fichiers suspects sont des fichiers détectés par l'analyse heuristique pouvant être infectés par des malwares et pour lesquels une signature n'a pas encore été publiée.

Lorsque des fichiers suspects seront détectés durant l'analyse, vous serez invité à les envoyer au laboratoire BitDefender. Cliquez sur **OK** pour envoyer ces fichiers aux laboratoires BitDefender pour une analyse plus approfondie.

18.2.6. Afficher les journaux d'analyse

Pour afficher les résultats de l'analyse une fois la tâche exécutée, faites un clic droit sur la tâche et sélectionnez **Afficher les journaux**. La fenêtre suivante apparaît:



Journaux

Vous pouvez consulter ici les fichiers de rapport générés à chaque fois que la tâche était exécutée. Pour chaque fichier, vous obtenez des informations sur l'état du processus d'analyse, la date et l'heure de l'analyse et un résumé des résultats de l'analyse.

Deux boutons sont disponibles :

- **Supprimer** - pour supprimer le journal d'analyse sélectionné.
- **Afficher** - pour voir le journal d'analyse sélectionné. Le journal d'analyse s'affichera dans votre navigateur Internet par défaut.

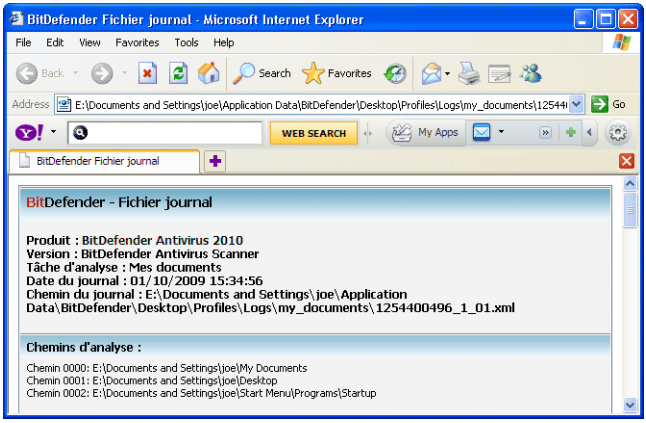
Note

Pour effacer ou visualiser un fichier, vous pouvez également faire un "clic-droit" sur le fichier et choisir l'option correspondante.

Cliquez sur **OK** pour sauvegarder les modifications et fermer la fenêtre. Pour lancer la tâche, cliquez sur **Analyser**.

Exemple de rapport d'analyse

La capture suivante représente un exemple d'un rapport d'analyse :


BitDefender Fichier journal - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address E:\Documents and Settings\joe\Application Data\BitDefender\Desktop\Profiles\Logs\my_documents\1254
Go
WEB SEARCH
My Apps
BitDefender Fichier journal
BitDefender - Fichier journal
Produit : BitDefender Antivirus 2010
Version : BitDefender Antivirus Scanner
Tâche d'analyse : Mes documents
Date du journal : 01/10/2009 15:34:56
Chemin du journal : E:\Documents and Settings\joe\Application Data\BitDefender\Desktop\Profiles\Logs\my_documents\1254400496_1_01.xml
Chemins d'analyse :
Chemin 0000: E:\Documents and Settings\joe\My Documents
Chemin 0001: E:\Documents and Settings\joe\Desktop
Chemin 0002: E:\Documents and Settings\joe\Start Menu\Programs\Startup

Exemple de rapport d'analyse

Le rapport d'analyse contient des informations détaillées sur le processus d'analyse, telles que les options d'analyse, la cible de l'analyse, les menaces trouvées et les actions prises sur ces menaces.

18.3. Objets exclus de l'analyse

Il peut arriver de devoir exclure certains fichiers de l'analyse. Par exemple, il peut être utile d'exclure un fichier test EICAR d'une analyse à l'accès ou des fichiers `.avi` d'une analyse sur demande.

BitDefender vous permet d'exclure des objets d'une analyse à l'accès ou d'une analyse sur demande ou des deux. Cette fonction permet de réduire la durée d'une analyse et d'éviter d'interférer dans votre travail.

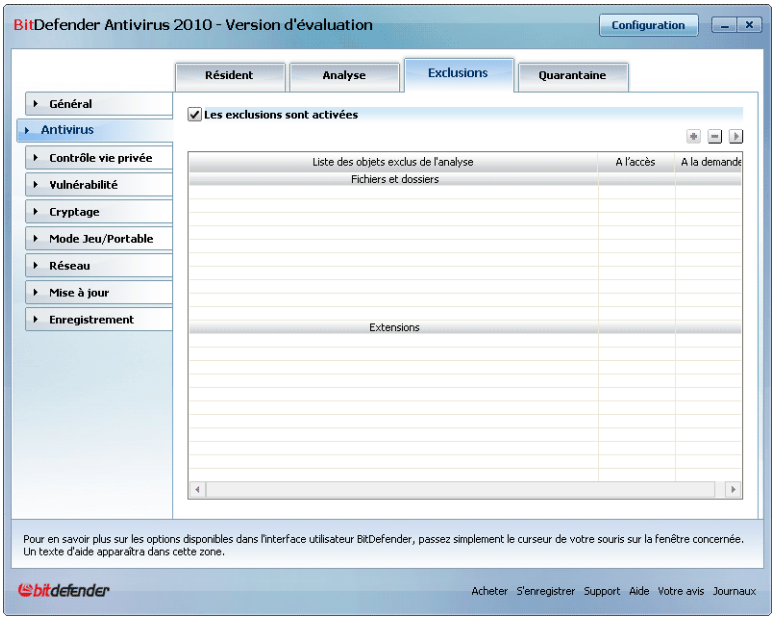
Deux types d'objet peuvent être exclus d'une analyse:

- **Chemins** - un fichier ou un dossier (avec tous les objets qu'il contient) indiqué par un chemin spécifique ;
- **Extensions** - tous les fichiers ayant une extension spécifique.

Note

Les objets exclus d'une analyse à l'accès ne sont pas analysés, que ce soit vous-même ou une application qui y accédiez.

Pour afficher et gérer les objets exclus de l'analyse, cliquez sur **Antivirus > Exceptions** en Mode Expert.



Exceptions

Les objets (fichiers, dossiers, extensions) exclus de l'analyse s'affichent. Il est indiqué pour chaque objet si celui-ci est exclus d'une analyse à l'accès, d'une analyse sur demande ou des deux.

Note

Les exceptions spécifiées ici ne s'appliquent PAS à l'analyse contextuelle. L'analyse contextuelle est un type d'analyse à la demande : vous faites un clic droit sur le fichier ou le dossier que vous souhaitez analyser et vous sélectionnez **Analyser avec BitDefender**.

Pour supprimer une entrée du tableau, sélectionnez-la et cliquez sur le bouton **Supprimer**.

Pour modifier une entrée du tableau, sélectionnez-la et cliquez sur le bouton **Modifier**. Une nouvelle fenêtre apparaît vous permettant de modifier l'extension ou le chemin à exclure et le type d'analyse dont vous souhaitez les exclure, le cas échéant. Effectuez les modifications nécessaires, puis cliquez sur **OK**.

Note

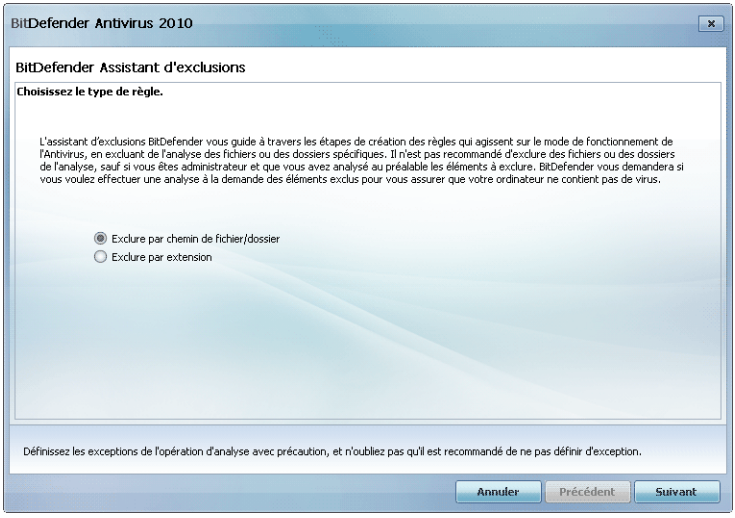
Vous pouvez aussi faire un clic droit sur un objet et utiliser les options du menu de raccourcis pour le modifier ou le supprimer.

Vous pouvez cliquer sur **Annuler** pour revenir aux modifications effectuées dans le tableau des règles, à condition que vous ne les ayez pas enregistrées en cliquant sur **Appliquer**.

18.3.1. Exclusion des chemins de l'analyse

Pour exclure des chemins de l'analyse, cliquez sur le bouton **Ajouter**. Vous serez guidé tout au long du processus d'exclusion par l'assistant de configuration qui apparaîtra.

Étape 1/4 - Sélectionner le type d'objet

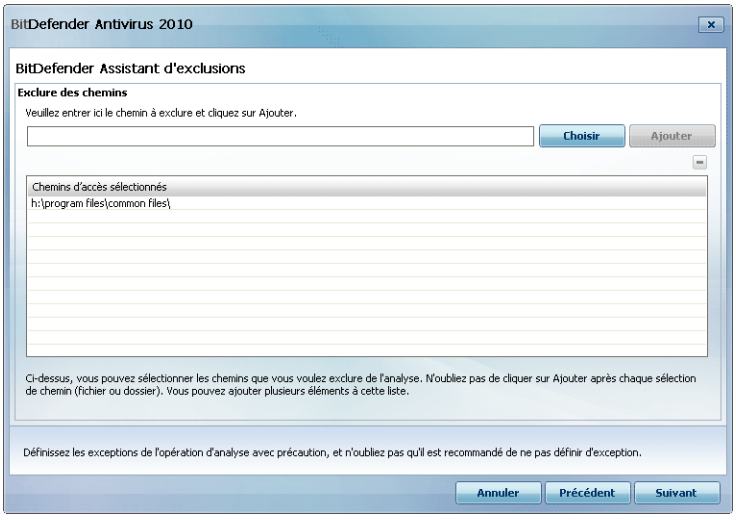

BitDefender Antivirus 2010
BitDefender Assistant d'exclusions
Choisissez le type de règle.
L'assistant d'exclusions BitDefender vous guide à travers les étapes de création des règles qui agissent sur le mode de fonctionnement de l'Antivirus, en excluant de l'analyse des fichiers ou des dossiers spécifiques. Il n'est pas recommandé d'exclure des fichiers ou des dossiers de l'analyse, sauf si vous êtes administrateur et que vous avez analysé au préalable les éléments à exclure. BitDefender vous demandera si vous voulez effectuer une analyse à la demande des éléments exclus pour vous assurer que votre ordinateur ne contient pas de virus.
Exclure par chemin de fichier/dossier
Exclure par extension
Définissez les exceptions de l'opération d'analyse avec précaution, et n'oubliez pas qu'il est recommandé de ne pas définir d'exception.
Annuler
Précédent
Suivant

Type d'objet

Sélectionnez l'option d'exclusion d'un chemin de l'analyse.

Cliquez sur **Suivant**.

Étape 2/4 - Spécifier les chemins à exclure


BitDefender Antivirus 2010
BitDefender Assistant d'exclusions
Exclure des chemins
Veuillez entrer ici le chemin à exclure et cliquez sur Ajouter.
Choisir
Ajouter
Chemins d'accès sélectionnés
h:\program files\common files\
Ci-dessus, vous pouvez sélectionner les chemins que vous voulez exclure de l'analyse. N'oubliez pas de cliquer sur Ajouter après chaque sélection de chemin (fichier ou dossier). Vous pouvez ajouter plusieurs éléments à cette liste.
Définissez les exceptions de l'opération d'analyse avec précaution, et n'oubliez pas qu'il est recommandé de ne pas définir d'exception.
Annuler
Précédent
Suivant

Chemins à exclure

Pour spécifier les chemins à exclure de l'analyse, utilisez l'une des méthodes suivantes :

- Cliquez sur **Parcourir**, sélectionnez le fichier ou le dossier à exclure de l'analyse, puis cliquez sur **Ajouter**.
- Saisissez le chemin à exclure de l'analyse dans la zone de texte, puis cliquez sur **Ajouter**.

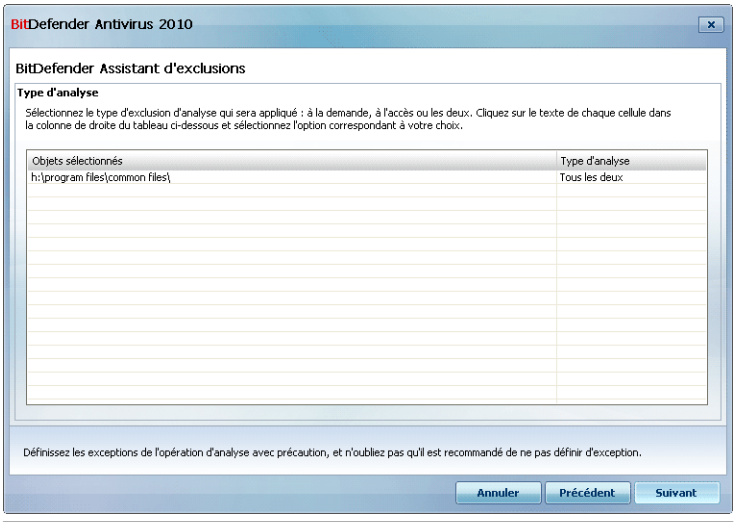
> **Note**
> Si le chemin indiqué n'existe pas, un message d'erreur apparaît. Cliquez sur **OK** et vérifiez la validité du chemin.

Les chemins apparaissent dans le tableau au fur et à mesure que vous les ajoutez. Vous pouvez en ajouter autant que vous le souhaitez.

Pour supprimer une entrée du tableau, sélectionnez-la et cliquez sur le bouton **Supprimer**.

Cliquez sur **Suivant**.

Étape 3/4 - Sélectionner le type d'analyse


BitDefender Antivirus 2010
BitDefender Assistant d'exclusions
Type d'analyse
Sélectionnez le type d'exclusion d'analyse qui sera appliqué : à la demande, à l'accès ou les deux. Cliquez sur le texte de chaque cellule dans la colonne de droite du tableau ci-dessous et sélectionnez l'option correspondant à votre choix.
Objets sélectionnés
Type d'analyse
h:\program files\common files\
Tous les deux
Définissez les exceptions de l'opération d'analyse avec précaution, et n'oubliez pas qu'il est recommandé de ne pas définir d'exception.
Annuler
Précédent
Suivant

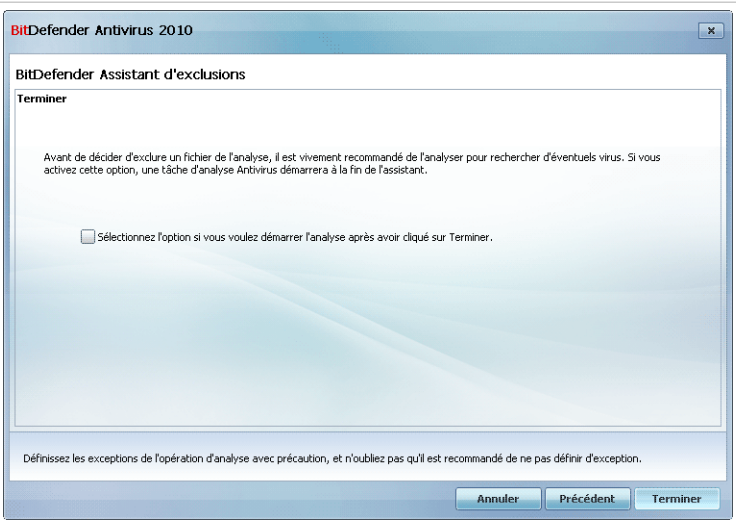
Type d'analyse

Un tableau contenant les chemins à exclure de l'analyse et le type d'analyse dont ils sont exclus est affiché.

Par défaut, les chemins sélectionnés sont exclus à la fois de l'analyse à l'accès et de l'analyse sur demande. Pour modifier quand appliquer l'exception, cliquez sur la colonne de droite et sélectionnez l'option souhaitée dans la liste.

Cliquez sur **Suivant**.

Étape 4/4 - Analyser les fichiers exclus


BitDefender Antivirus 2010
BitDefender Assistant d'exclusions
Terminer
Avant de décider d'exclure un fichier de l'analyse, il est vivement recommandé de l'analyser pour rechercher d'éventuels virus. Si vous activez cette option, une tâche d'analyse Antivirus démarrera à la fin de l'assistant.
Sélectionnez l'option si vous voulez démarrer l'analyse après avoir cliqué sur Terminer.
Définissez les exceptions de l'opération d'analyse avec précaution, et n'oubliez pas qu'il est recommandé de ne pas définir d'exception.
Annuler
Précédent
Terminer

Analyser les fichiers exclus

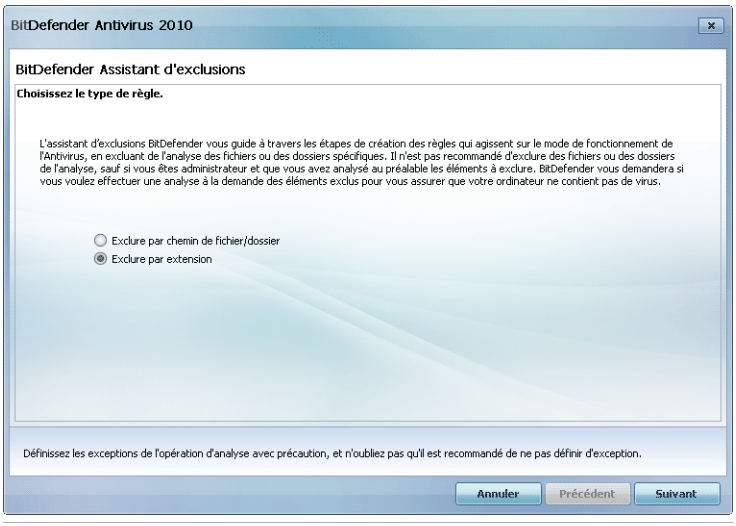
Il vous est fortement conseillé d'analyser les fichiers dans les chemins spécifiés pour vous assurer qu'ils ne soient pas infectés. Cochez la case pour analyser ces fichiers avant de les exclure de l'analyse.

Cliquez sur **Terminer**.

18.3.2. Exclusion des extensions de l'analyse

Pour exclure des extensions de l'analyse, cliquez sur le bouton **Ajouter**. Vous serez guidé tout au long du processus d'exclusion par l'assistant de configuration qui apparaîtra.

Étape 1/4 - Sélectionner le type d'objet

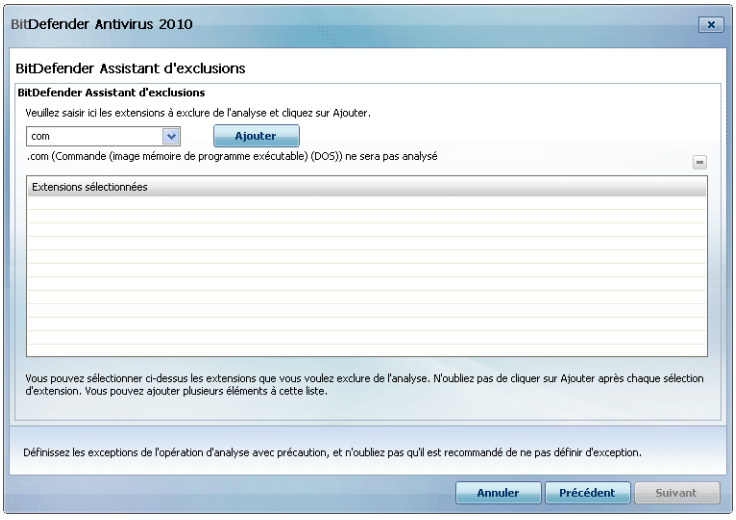

BitDefender Antivirus 2010
BitDefender Assistant d'exclusions
Choisissez le type de règle.
L'assistant d'exclusions BitDefender vous guide à travers les étapes de création des règles qui agissent sur le mode de fonctionnement de l'Antivirus, en excluant de l'analyse des fichiers ou des dossiers spécifiques. Il n'est pas recommandé d'exclure des fichiers ou des dossiers de l'analyse, sauf si vous êtes administrateur et que vous avez analysé au préalable les éléments à exclure. BitDefender vous demandera si vous voulez effectuer une analyse à la demande des éléments exclus pour vous assurer que votre ordinateur ne contient pas de virus.
Exclure par chemin de fichier/dossier
Exclure par extension
Définissez les exceptions de l'opération d'analyse avec précaution, et n'oubliez pas qu'il est recommandé de ne pas définir d'exception.
Annuler
Précédent
Suivant

Type d'objet

Sélectionnez l'option d'exclusion d'extensions de l'analyse.

Cliquez sur **Suivant**.

Étape 2/4 - Spécifier les extensions exclues


BitDefender Antivirus 2010
BitDefender Assistant d'exclusions
BitDefender Assistant d'exclusions
Veuillez saisir ici les extensions à exclure de l'analyse et cliquez sur Ajouter.
com
Ajouter
.com (Commande (image mémoire de programme exécutable) (DOS)) ne sera pas analysé
Extensions sélectionnées
Vous pouvez sélectionner ci-dessus les extensions que vous voulez exclure de l'analyse. N'oubliez pas de cliquer sur Ajouter après chaque sélection d'extension. Vous pouvez ajouter plusieurs éléments à cette liste.
Définissez les exceptions de l'opération d'analyse avec précaution, et n'oubliez pas qu'il est recommandé de ne pas définir d'exception.
Annuler
Précédent
Suivant

Extensions à exclure

Pour spécifier les extensions à exclure de l'analyse, utilisez l'une des méthodes suivantes :

- Sélectionnez dans le menu l'extension que vous souhaitez exclure de l'analyse, puis cliquez sur **Ajouter**.

> **Note**
> Le menu contient la liste de toutes les extensions enregistrées dans votre système. Lorsque vous sélectionnez une extension, sa description s'affiche si elle est disponible.

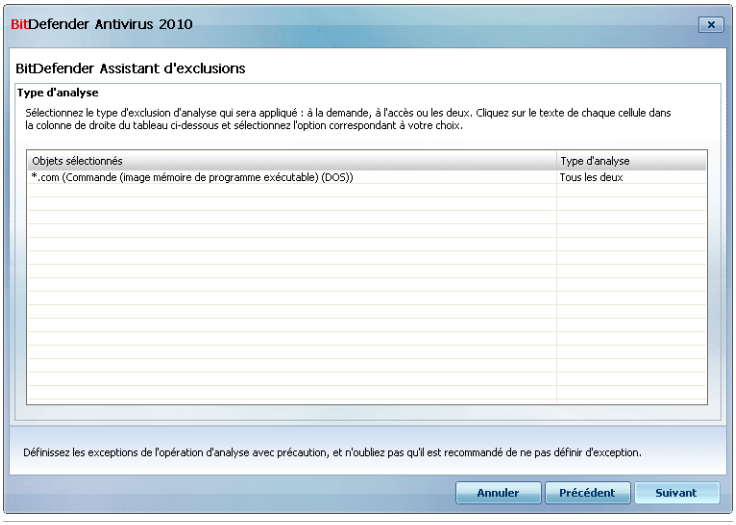
- Saisissez l'extension à exclure de l'analyse dans la zone de texte, puis cliquez sur **Ajouter**.

Les extensions apparaissent dans le tableau au fur et à mesure que vous les ajoutez. Vous pouvez en ajouter autant que vous le souhaitez.

Pour supprimer une entrée du tableau, sélectionnez-la et cliquez sur le bouton **Supprimer**.

Cliquez sur **Suivant**.

Étape 3/4 - Sélectionner le type d'analyse


BitDefender Antivirus 2010
BitDefender Assistant d'exclusions
Type d'analyse
Sélectionnez le type d'exclusion d'analyse qui sera appliqué : à la demande, à l'accès ou les deux. Cliquez sur le texte de chaque cellule dans la colonne de droite du tableau ci-dessous et sélectionnez l'option correspondant à votre choix.
Objets sélectionnés
Type d'analyse
*.com (Commande (image mémoire de programme exécutable) (DOS))
Tous les deux
Définissez les exceptions de l'opération d'analyse avec précaution, et n'oubliez pas qu'il est recommandé de ne pas définir d'exception.
Annuler
Précédent
Suivant

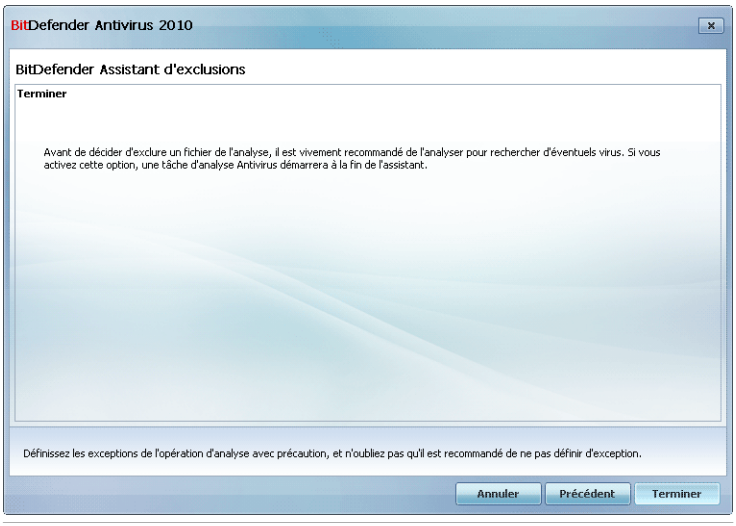
Type d'analyse

Un tableau s'affiche contenant les extensions devant être exclues de l'analyse et le type d'analyse dont elles sont exclues.

Par défaut, les extensions sélectionnées sont exclues à la fois de l'analyse à l'accès et de l'analyse sur demande. Pour modifier quand appliquer l'exception, cliquez sur la colonne de droite et sélectionnez l'option souhaitée dans la liste.

Cliquez sur **Suivant**.

Étape 4/4 - Sélectionner le type d'analyse


BitDefender Antivirus 2010
BitDefender Assistant d'exclusions
Terminer
Avant de décider d'exclure un fichier de l'analyse, il est vivement recommandé de l'analyser pour rechercher d'éventuels virus. Si vous activez cette option, une tâche d'analyse Antivirus démarrera à la fin de l'assistant.
Définissez les exceptions de l'opération d'analyse avec précaution, et n'oubliez pas qu'il est recommandé de ne pas définir d'exception.
Annuler
Précédent
Terminer

Type d'analyse

Il est fortement conseillé d'analyser les fichiers comportant les extensions spécifiées pour vous assurer qu'ils ne soient pas infectés.

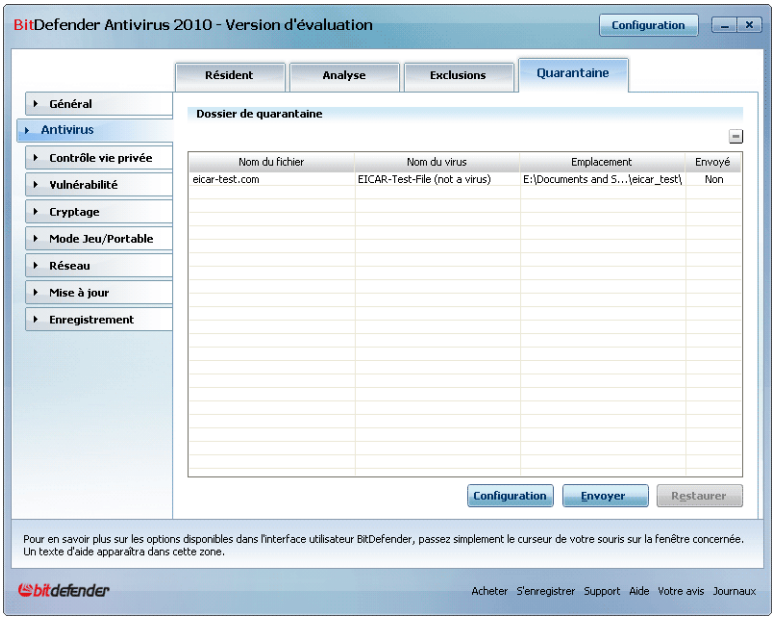
Cliquez sur **Terminer**.

18.4. Zone de quarantaine

BitDefender permet d'isoler les fichiers infectés ou suspects dans une zone sécurisée, nommée quarantaine. En isolant ces fichiers dans la quarantaine, le risque d'être infecté disparaît et, en même temps, vous avez la possibilité d'envoyer ces fichiers pour une analyse par le VirusLab de BitDefender.

BitDefender analyse également les fichiers en quarantaine après chaque mise à jour de signatures de malware. Les fichiers nettoyés sont automatiquement remis à leur emplacement d'origine.

Pour afficher et gérer les fichiers en quarantaine et pour configurer les paramètres de la quarantaine, cliquez sur **Antivirus > Quarantaine** en Mode Expert.



Quarantaine

La partie Quarantaine affiche tous les fichiers actuellement isolés dans le dossier Quarantaine. Pour chaque fichier en quarantaine, vous pouvez voir son nom, le nom du virus détecté, le chemin de son emplacement d'origine et sa date de soumission.

Note
Quand un virus est en quarantaine, il ne peut faire aucun dégât car il ne peut ni être exécuté ni lu.

18.4.1. Gérer les fichiers en quarantaine

Vous pouvez envoyer un fichier depuis la quarantaine aux BitDefender Labs en cliquant sur **Envoyer**. Par défaut, BitDefender soumettra automatiquement toutes les heures les fichiers mis en quarantaine.

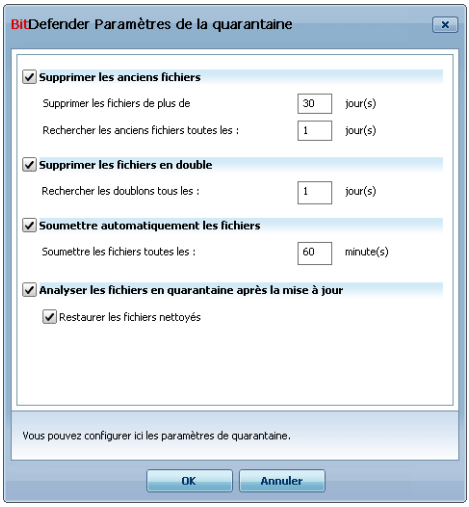
Pour supprimer un fichier sélectioné dans la zone de quarantaine, cliquez sur le bouton **Supprimer**. Si vous voulez restaurer un fichier sélectionné dans son emplacement d'origine, cliquez sur **Restaurer**.

Menu contextuel. Le menu contextuel qui vous est proposé vous permet de gérer facilement les fichiers en quarantaine. Les options disponibles sont les mêmes que

celles mentionnées précédemment. Vous pouvez aussi sélectionner **Actualiser** pour rafraîchir la zone de quarantaine.

18.4.2. Configuration des paramètres de la quarantaine

Pour configurer les paramètres de la quarantaine, cliquez sur **Paramètres**. Une nouvelle fenêtre s'affiche.



Paramètres de la quarantaine

En utilisant les paramètres de la quarantaine, vous pouvez configurer BitDefender pour exécuter automatiquement les actions suivantes :

Supprimer les anciens fichiers. Pour supprimer automatiquement les anciens fichiers en quarantaine, cochez l'option correspondante. Vous devez spécifier après combien de jours les fichiers en quarantaine doivent être supprimés et la fréquence à laquelle BitDefender doit rechercher les anciens fichiers.

Note
Par défaut, BitDefender recherche les anciens fichiers chaque jour et supprime les fichiers de plus de 30 jours.

Supprimer les fichiers en double. Pour supprimer automatiquement les doublons de fichiers en quarantaine, cochez l'option correspondante. Vous devez spécifier le nombre de jours entre deux recherches consécutives de doublons.

Note

Par défaut, BitDefender recherche les doublons de fichiers en quarantaine chaque jour.

Soumettre automatiquement les fichiers. Pour soumettre automatiquement les fichiers en quarantaine, cochez l'option correspondante. Vous devez spécifier la fréquence à laquelle soumettre les fichiers.

Note

Par défaut, BitDefender soumettra automatiquement toutes les heures les fichiers mis en quarantaine.

Analyser les fichiers en quarantaine après une mise à jour. Pour analyser automatiquement les fichiers en quarantaine après chaque mise à jour effectuée, cochez l'option correspondante. Vous pouvez choisir de remettre automatiquement vos fichiers sains dans leur emplacement d'origine en sélectionnant **Restaurer les fichiers sains**.

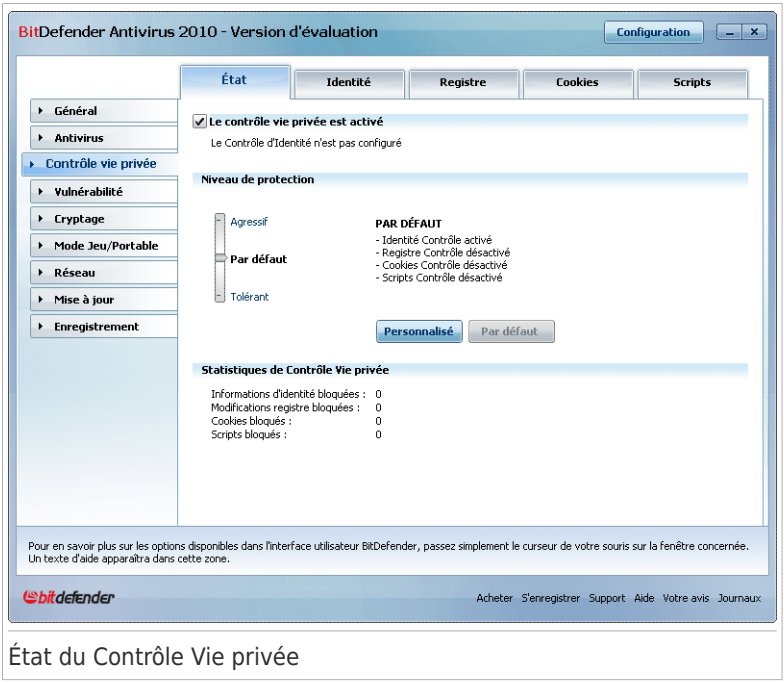
Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

19. Contrôle vie privée

BitDefender contrôle des dizaines de “points à risque” dans votre système où les spywares pourraient agir, et analyse également les modifications apportées à votre système et à vos logiciels. C’est efficace contre les chevaux de Troie et autres outils installés par des hackers, qui essaient de compromettre votre vie privée et d’envoyer vos informations personnelles, comme vos numéros de carte bancaire, de votre ordinateur vers le pirate.

19.1. État du Contrôle Vie privée

Pour configurer le Contrôle Vie privée et consulter des informations sur son activité, allez dans **Contrôle Vie privée>État** en Mode Expert.



État du Contrôle Vie privée

Vous pouvez vérifier si le Contrôle Vie privée est activé ou désactivé. Si vous voulez modifier l'état du Contrôle Vie privée, cochez ou décochez la case correspondante.

Important

Pour prévenir le vol d'informations et protéger votre vie privée, laissez le module **Contrôle Vie Privée** activé.

Le Contrôle Vie privée protège votre ordinateur en effectuant ces contrôles de protection essentiels :

- Contrôle d'identité - protège vos données confidentielles en filtrant tout le trafic sortant Internet (HTTP), e-mail (SMTP) et de messagerie instantanée selon les règles que vous avez créées dans la section Identité.
- Contrôle de la base de registre - demande votre autorisation dès lors qu'un programme tente de modifier une entrée de registre afin de s'exécuter au démarrage de Windows.
- Contrôle des cookies - demande votre autorisation dès lors qu'un nouveau site Web tente de créer un cookie sur votre ordinateur.
- Contrôle des scripts - demande votre autorisation dès lors qu'un site Web tente d'exécuter un script ou un autre contenu actif.

En bas de la section, vous pouvez consulter les **statistiques du Contrôle Vie privée**.

19.1.1. Configuration du niveau de protection

Vous pouvez choisir le niveau de protection qui répond le mieux à vos besoins de sécurité. Déplacez le curseur sur l'échelle pour choisir le niveau approprié.

Il existe trois niveaux de protection:

Niveau de protection	Description
Tolérant	Tous les contrôles de protection sont désactivés.
Par défaut	Seul le **Contrôle d'Identité** est activé.
Agressif	**Contrôle d'Identité**, **Contrôle du Registre**, **Contrôle des Cookies** et **Contrôle des Scripts** sont activés.

Vous pouvez personnaliser le niveau de protection en cliquant sur **Personnaliser**. Dans la fenêtre qui apparaîtra, sélectionnez les contrôles de protection que vous souhaitez activer et cliquez sur **OK**.

Cliquez sur **Niveau par défaut** pour placer le curseur sur le niveau par défaut.

19.2. Contrôle d'identité

La protection des données confidentielles est un sujet important qui nous concerne tous. Le vol d'informations a suivi le développement de l'Internet et des communications et utilise de nouvelles méthodes pour pousser les gens à communiquer leurs données privées.

Qu'il s'agisse de votre adresse email ou de votre numéro de carte bancaire, si ces informations tombent dans de mauvaises mains vous pouvez en subir les conséquences: crouler sous le spam ou retrouver votre compte bancaire vide.

Le contrôle d'identité vous protège contre le vol de données sensibles lorsque vous êtes connecté à Internet. En se basant sur les règles définies par vous-même, le contrôle d'identité analyse le trafic Internet, de messagerie et de messagerie instantanée partant de votre ordinateur, pour y rechercher des chaînes de texte spécifiques que vous avez définies (par exemple, votre numéro de carte de crédit). En cas de correspondance, la page Web, l'e-mail ou l'échange de messagerie instantanée concerné est bloqué.

Vous pouvez créer des règles pour protéger toutes les informations que vous considérez comme personnelles ou confidentielle, votre numéro de téléphone, votre adresse e-mail ou votre Numéro de compte bancaire... Le support multi-utilisateurs est fourni pour que les utilisateurs connectés sur des comptes Windows différents puissent configurer et utiliser leurs propres règles de protection. Si votre compte Windows est un compte administrateur, les règles que vous créez peuvent être configurées pour s'appliquer également lorsque d'autres utilisateurs de l'ordinateur sont connectés à leurs comptes utilisateurs Windows.

Pourquoi utiliser le Contrôle d'identité?

- Le Contrôle d'identité est très efficace dans le blocage des spywares keylogger. Ce type d'applications malicieuses enregistre vos frappes clavier et les envoie par Internet à des pirates. Le pirate peut récupérer des informations sensibles à partir des données volées, comme vos numéros de comptes bancaires ou vos mots de passe pour les utiliser à son propre profit.

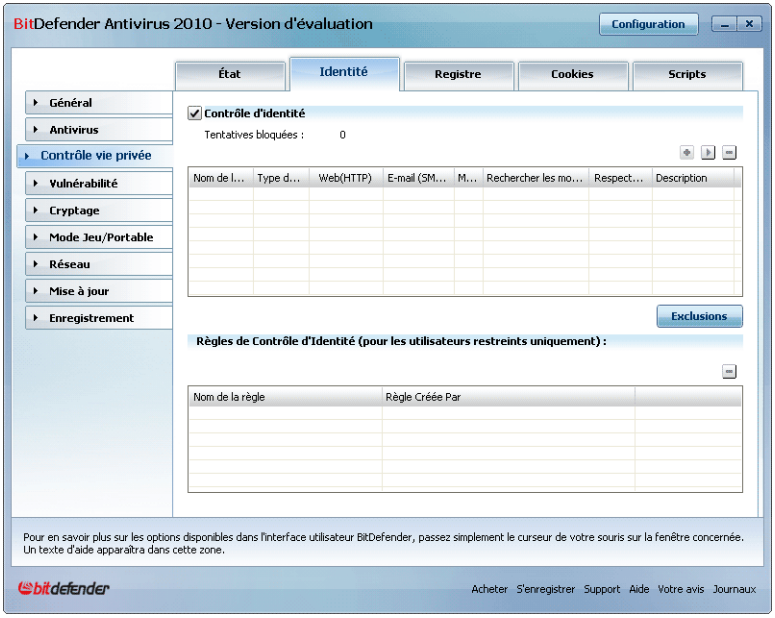
  Dans l'hypothèse où une application de ce type réussirait à contourner la protection antivirus, elle ne pourra pas envoyer les données subtilisées par email, par le web ou par messagerie instantanée si vous avez créé les règles de protection d'identité adaptées.

- Le Contrôle d'identité peut vous protéger contre les tentatives de phishing (Attaques visant à voler les informations personnelles). La technique la plus répandue lors des tentatives de Phishing est l'envoi d'un email trompeur visant à vous amener à communiquer vos informations personnelles sur une fausse page Web.

  Par exemple, vous pouvez recevoir un email prétendument de votre banque vous demandant de mettre à jour rapidement vos informations bancaires. Cet email vous propose de cliquer sur un lien vous redirigeant vers une page Web sur laquelle vous devez communiquer vos informations personnelles. Bien qu'ils aient l'air légitimes, le lien de redirection et la page Web vers laquelle vous êtes redirigé sont faux. Si vous cliquez sur le lien contenu dans l'email et que vous entrez vos informations personnelles sur la fausse page web, vous divulguerez ces informations au pirate qui est l'auteur de cette tentative de phishing.

Si les règles de protection d'identité sont actives, vous ne pourrez pas soumettre d'information personnelle sur une page Web (comme votre Numéro de carte de crédit par exemple) sauf si vous avez explicitement définit cette page comme étant autorisée à recevoir ce type d'information.

Pour configurer le contrôle d'identité, allez dans **Contrôle Vie privée>Identité** en Mode Expert.



Contrôle d'identité

Pour utiliser le contrôle d'identité, suivez les étapes indiquées :

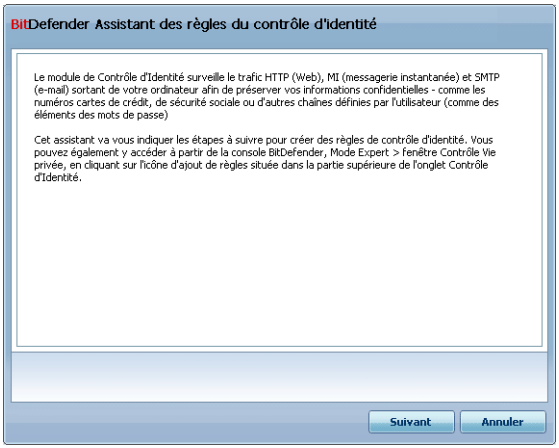
1. Cochez la case **Activer le Contrôle d'identité**.
2. Définissez les règles nécessaires à la protection de vos données sensibles. Pour plus d'informations, reportez-vous à « *Création de règles d'Identité* » (p. 159).
3. Définissez si nécessaire des exceptions aux règles que vous avez créées. Pour plus d'informations, reportez-vous à « *Définition des Exceptions* » (p. 162).
4. Si vous êtes un administrateur de cet ordinateur, vous pouvez vous exclure des règles d'identité créées par d'autres administrateurs.

   Pour plus d'informations, reportez-vous à « *Règles Définies par d'Autres Administrateurs* » (p. 164).

19.2.1. Création de règles d'Identité

Pour créer une règle de protection de l'identité, clique sur le bouton **Ajouter** et suivez les instructions de l'assistant de configuration.

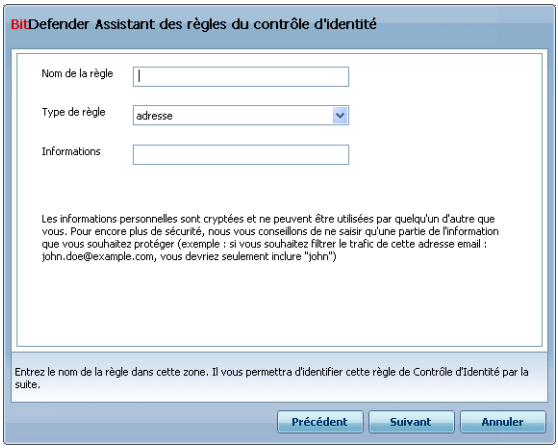
Etape 1 sur 4- Fenêtre d'accueil


BitDefender Assistant des règles du contrôle d'identité
Le module de Contrôle d'Identité surveille le trafic HTTP (Web), MI (messagerie instantanée) et SMTP (e-mail) sortant de votre ordinateur afin de préserver vos informations confidentielles - comme les numéros cartes de crédit, de sécurité sociale ou d'autres chaînes définies par l'utilisateur (comme des éléments des mots de passe)
Cet assistant va vous indiquer les étapes à suivre pour créer des règles de contrôle d'identité. Vous pouvez également y accéder à partir de la console BitDefender, Mode Expert > fenêtre Contrôle Vie privée, en cliquant sur l'icône d'ajout de règles située dans la partie supérieure de l'onglet Contrôle d'Identité.
Suivant
Annuler

Page d'accueil

Cliquez sur **Suivant**.

Étape 2/4 - Définir le type de règle et les données


BitDefender Assistant des règles du contrôle d'identité
Nom de la règle
Type de règle
adresse
Informations
Les informations personnelles sont cryptées et ne peuvent être utilisées par quelqu'un d'autre que vous. Pour encore plus de sécurité, nous vous conseillons de ne saisir qu'une partie de l'information que vous souhaitez protéger (exemple : si vous souhaitez filtrer le trafic de cette adresse email : john.doe@example.com, vous devriez seulement inclure "john")
Entrez le nom de la règle dans cette zone. Il vous permettra d'identifier cette règle de Contrôle d'Identité par la suite.
Précédent
Suivant
Annuler

Définition des types de règles et de données

Vous devez définir les paramètres suivants:

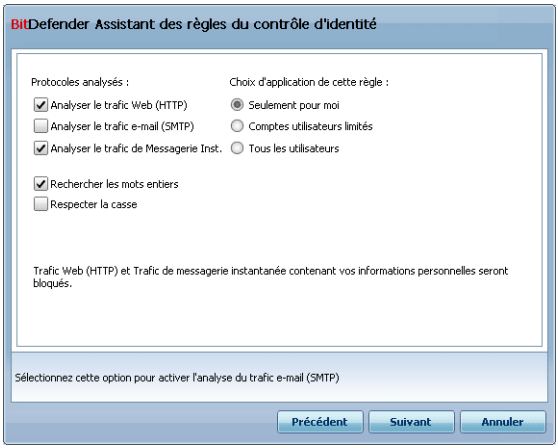
- **Nom de la règle** - saisissez le nom de la règle dans ce champ de saisie.
- **Type de règle** - détermine le type de règle (addresse, nom, carte de crédit, code PIN, etc.)
- **Données de la règle** - saisissez les données que vous voulez protéger dans ce champ de saisie. Si par exemple vous voulez protéger votre numéro de carte de crédit, saisissez ici l'intégralité ou une partie de celui-ci.

> **Note**
> Si vous saisissez moins de trois caractères, vous serez invité à valider les données. Nous vous recommandons de saisir au moins trois caractères afin d'éviter le blocage erroné de messages et de pages Web.

Toutes les données que vous enregistrez sont cryptées. Pour plus de sécurité, n'entrez pas toutes les données que vous souhaitez protéger.

Cliquez sur **Suivant**.

Étape 3/4 - Sélectionner les types de trafic et les utilisateurs


BitDefender Assistant des règles du contrôle d'identité
Protocoles analysés :
Analyser le trafic Web (HTTP)
Analyser le trafic e-mail (SMTP)
Analyser le trafic de Messagerie Inst.
Rechercher les mots entiers
Respecter la casse
Choix d'application de cette règle :
Seulement pour moi
Comptes utilisateurs limités
Tous les utilisateurs
Trafic Web (HTTP) et Trafic de messagerie instantanée contenant vos informations personnelles seront bloqués.
Sélectionnez cette option pour activer l'analyse du trafic e-mail (SMTP)
Précédent
Suivant
Annuler

Sélectionnez les types de trafic et les utilisateurs

Sélectionnez le type de trafic que BitDefender doit analyser. Voici les options proposées :

- **Analyse Web (trafic HTTP)** - analyse le trafic Web (HTTP) et bloque les données sortantes correspondant aux données de la règle.
- **Analyse e-mail (trafic SMTP)** - analyse le trafic mail (SMTP) et bloque les e-mails sortants qui contiennent les éléments déterminés dans la règle de gestion des données.
- **Analyse du trafic de Messagerie Instantanée** - analyse le trafic de Messagerie Instantanée et bloque les échanges sortants qui contiennent les éléments déterminés dans la règle de gestion des données.

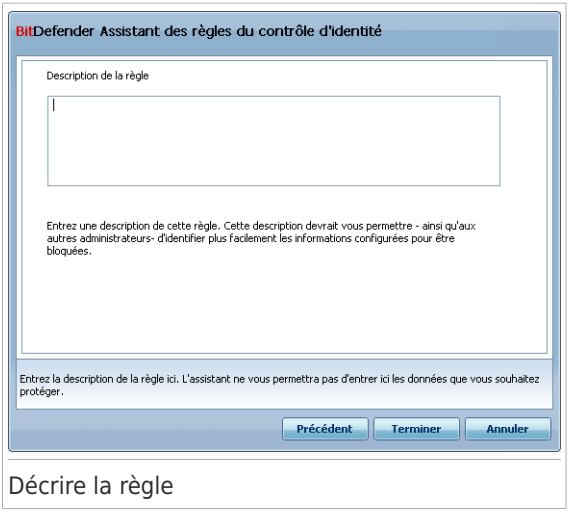
Vous pouvez choisir d'appliquer la règle uniquement si les données de la règle correspondent à tous les mots ou à la chaîne de caractères détectée.

Spécifiez les utilisateurs pour lesquels la règle s'applique.

- **Seulement pour moi (utilisateur actuel)** - la règle s'appliquera seulement à votre compte utilisateur.
- **Comptes utilisateurs limités** - la règle s'appliquera à vous et aux comptes Windows limités.
- **Tous les utilisateurs** - la règle s'appliquera à tous les comptes Windows.

Cliquez sur **Suivant**.

Étape 4/4 - Décrire la règle


BitDefender Assistant des règles du contrôle d'identité
Description de la règle
Entrez une description de cette règle. Cette description devrait vous permettre - ainsi qu'aux autres administrateurs- d'identifier plus facilement les informations configurées pour être bloquées.
Entrez la description de la règle ici. L'assistant ne vous permettra pas d'entrer ici les données que vous souhaitez protéger.
Précédent
Terminer
Annuler

Décrire la règle

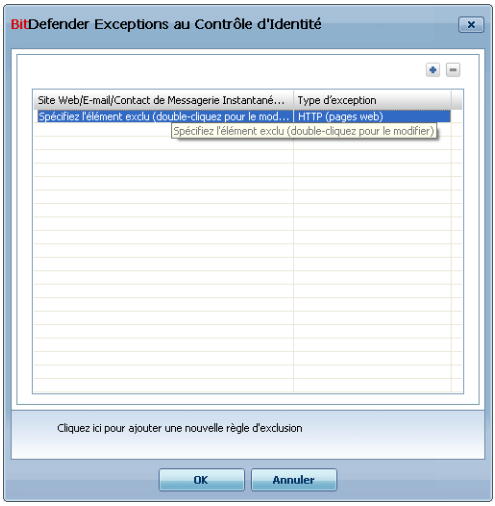
Entrez une description courte de la règle dans le champ correspondant. Puisque les données bloquées (chaines de caractères) ne sont pas affichées sous forme de texte clair quand vous accédez à la règle, la description devrait vous aider à l'identifier rapidement.

Cliquez sur **Terminer**. La règle apparaîtra dans le tableau.

19.2.2. Définition des Exceptions

Il y a certains cas où vous avez besoin de définir des exceptions à des règles d'identité spécifiques. Si vous créez, par exemple, une règle de confidentialité pour éviter que votre numéro de carte de crédit ne soit envoyé via HTTP (Web), chaque fois que le numéro de votre carte sera soumis sur un site Web depuis votre compte utilisateur, la page correspondante sera bloquée. Si vous voulez, par exemple, acheter des chaussures sur une boutique en ligne (que vous savez fiable), vous devrez spécifier une exception à la règle correspondante.

Pour ouvrir la fenêtre permettant de gérer les exceptions, cliquez sur **Exceptions**.


BitDefender Exceptions au Contrôle d'Identité
Site Web/E-mail/Contact de Messagerie Instantané...
Type d'exception
Spécifiez l'élément exclu (double-cliquez pour le mod...
HTTP (pages web)
Spécifiez l'élément exclu (double-cliquez pour le modifier)
Cliquez ici pour ajouter une nouvelle règle d'exclusion
OK
Annuler

Exclusions

Pour ajouter une exception, procédez comme suit :

1. Cliquez sur le bouton **Ajouter** pour ajouter une nouvelle entrée au tableau.
2. Double-cliquez sur **Indiquer l'élément à exclure** et précisez le site Web, l'adresse e-mail ou le contact de messagerie instantanée que vous souhaitez ajouter comme exception.
3. Double-cliquez sur **Type de trafic** et sélectionnez dans le menu l'option correspondant au type d'adresse précédemment indiqué.
   - Si vous avez indiqué une adresse Web, sélectionnez **HTTP**.
   - Si vous avez indiqué une adresse e-mail, sélectionnez **E-mail (SMTP)**.
   - Si vous avez indiqué un contact de messagerie instantanée, sélectionnez **Messagerie instantanée**.

Pour supprimer une exception de la liste, sélectionnez-la et cliquez sur le bouton **Supprimer**.

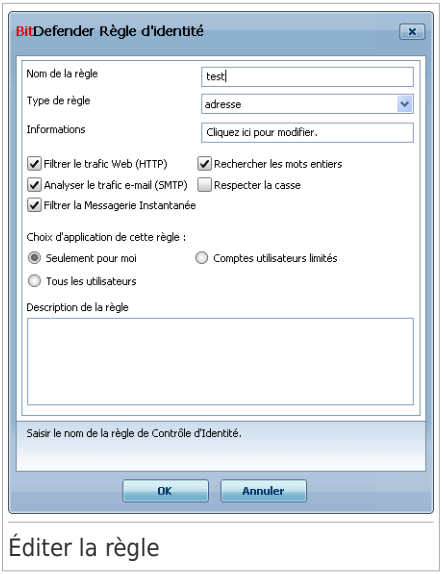
Cliquez **OK** pour sauvegarder les changements.

19.2.3. Gestion des règles

Vous pouvez voir les règles existantes dans le tableau.

Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton **Supprimer**.

Pour modifier une règle, sélectionnez-la, puis cliquez sur le bouton **Modifier**, ou double-cliquez dessus. Une nouvelle fenêtre s'affiche alors.



Éditer la règle

Dans cette rubrique, vous pouvez modifier le nom, la description et les paramètres de la règle (type, données et trafic). Cliquez sur **OK** pour enregistrer les modifications.

19.2.4. Règles Définies par d'Autres Administrateurs

Lorsque vous n'êtes pas le seul utilisateur à disposer des droits administrateur sur votre système, les autres administrateurs peuvent aussi créer des règles d'identité. Si vous ne souhaitez pas que des règles créées par d'autres utilisateurs s'appliquent lorsque vous êtes connecté(e), BitDefender vous permet de vous exclure de toute règle que vous n'avez pas créée.

Vous pouvez voir une liste de règles créées par d'autres administrateurs dans le tableau sous **Règles de Contrôle d'Identité**. Pour chaque règle figurent dans le tableau son nom et l'utilisateur l'ayant créée.

Pour qu'une règle ne s'applique pas à vous-même, sélectionnez la règle dans le tableau et cliquez sur le bouton **Supprimer**.

19.3. Contrôle du registre

Une partie très importante du système d'exploitation Windows est appelée la **Base de registres**. C'est l'endroit où Windows conserve ses paramétrages, programmes installés, informations sur l'utilisateur et autres.

La **Base de registres** est également utilisée pour définir quels programmes devraient être lancés automatiquement lorsque Windows démarre. Cela est souvent utilisé par les virus afin d'être automatiquement lancé lorsque l'utilisateur redémarre son ordinateur.

Le **Contrôle des registres** garde un oeil sur les registres Windows – c'est également utile pour détecter des chevaux de Troie. Il vous alertera dès qu'un programme essaiera de modifier une entrée dans la base de registres afin de s'exécuter au démarrage de Windows.

BitDefender Alerte Contrôle Registre
test_vbscript.exe
va(vont) être ajouté(s) à la base de registre Windows
Chemin de l'application :
H:\Documents and Settings\amirea\Desktop\test_vbscript.exe
Si vous connaissez ce programme, vous pouvez autoriser cette action.
Autoriser
Bloquer

Alerte registres

Vous pouvez voir le programme essayant de modifier le registre Windows.

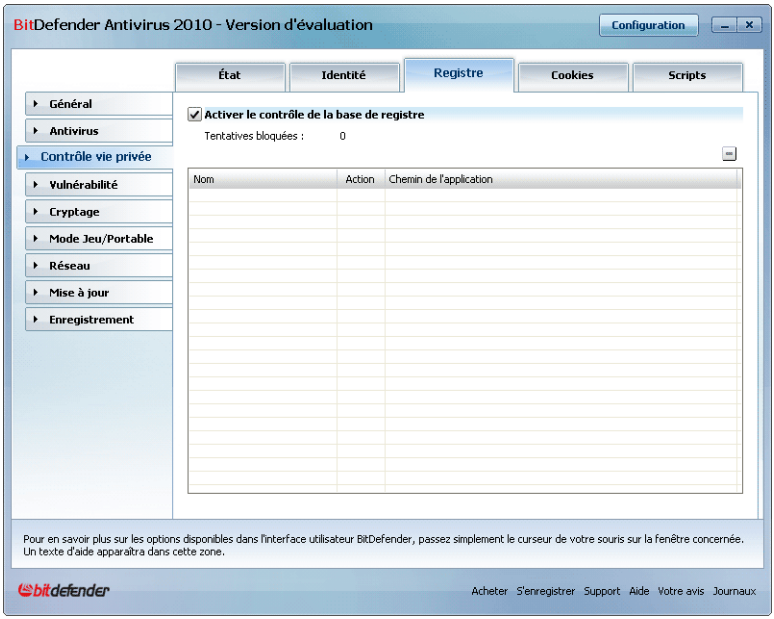
Si vous ne reconnaissez pas le programme et qu'il vous semble suspect, cliquez sur **Bloquer** pour l'empêcher de modifier le registre Windows. Autrement, cliquez sur **Autoriser** pour permettre la modification.

Une règle est créée et ajoutée au tableau des règles à partir de votre réponse. La même action est appliquée à chaque fois que ce programme tente de modifier une entrée de la base registre.

Note

BitDefender vous alertera à l'installation de nouveaux logiciels nécessitant d'être lancé après le prochain démarrage de votre ordinateur. Dans la plupart des cas, ces programmes sont légitimes et peuvent être autorisés.

Pour configurer le contrôle du registre, allez dans **Contrôle Vie privée> Registre** en Mode Expert.



Contrôle du registre

Vous pouvez voir les règles existantes dans le tableau.

Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton **Supprimer**.

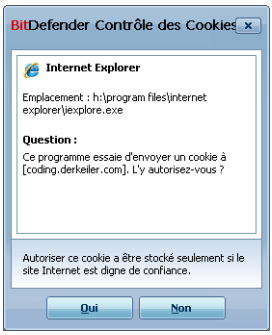
19.4. Contrôle des cookies

Les Cookies sont très communs sur Internet. Ce sont des petits fichiers stockés sur le PC. Les sites web les créent afin de connaître certaines informations vous concernant.

Les Cookies sont généralement là pour vous rendre la vie plus facile. Par exemple ils peuvent aider un site web se rappeler votre nom et vos préférences, pour ne pas avoir à les introduire chaque fois.

Mais les cookies peuvent aussi être utilisés pour compromettre votre confidentialité, en surveillant vos préférences de navigation.

C'est là qu'intervient **Contrôle des cookies**. Si activé, **Contrôle des cookies** demandera votre permission quand un site essaye d'établir un cookie localement:


BitDefender Contrôle des Cookies
Internet Explorer
Emplacement : h:\program files\internet explorer\iexplore.exe
Question :
Ce programme essaie d'envoyer un cookie à [coding.derkeiler.com]. L'y autorisez-vous ?
Autoriser ce cookie a être stocké seulement si le site Internet est digne de confiance.
Oui
Non

Alerte cookies suspects

Vous pouvez voir le nom de l'application qui tente de transmettre le fichier de type cookie.

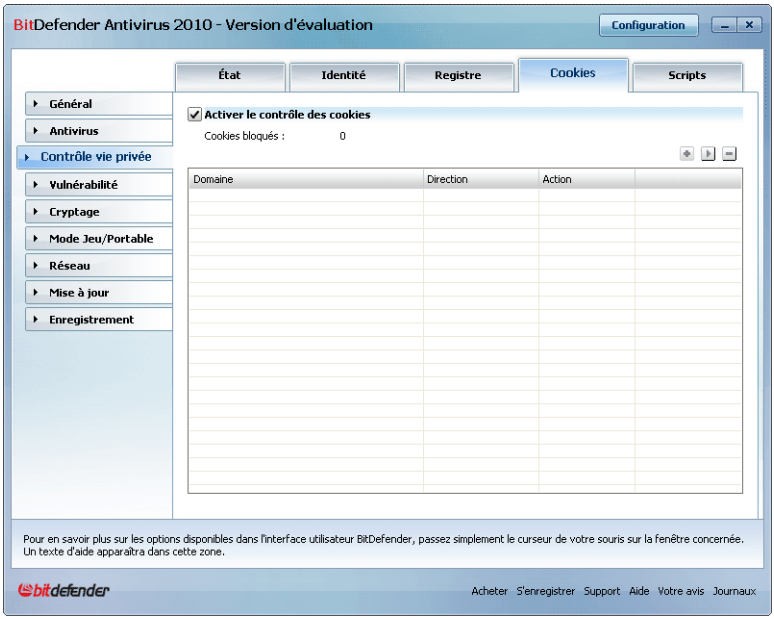
Cliquez sur **Oui** ou sur **Non** et une règle sera créée, appliquée, et ajoutée au tableau des règles.

Ceci vous aide à choisir à quels sites faire confiance et quels sites éviter.

Note

A cause du grand nombre de cookies utilisés sur Internet, **Cookie Control** peut être gênant au début. Il vous posera beaucoup de questions concernant les sites qui veulent placer des cookies sur votre ordinateur. Au fur et à mesure que vous rajoutez vos sites habituels à la liste des règles, la navigation deviendra aussi simple qu'avant.

Pour configurer le contrôle des cookies, allez dans **Contrôle Vie privée> Cookie** en Mode Expert.



Contrôle des cookies

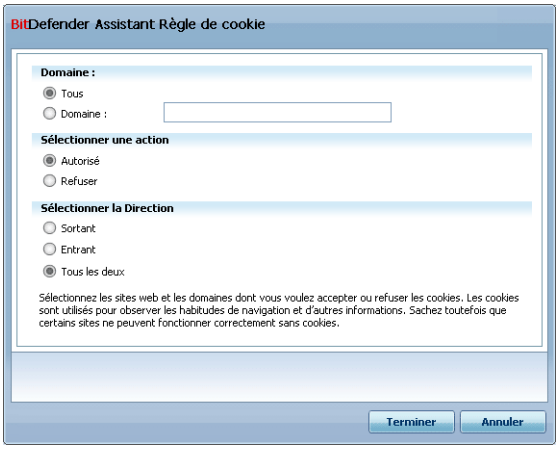
Vous pouvez voir les règles existantes dans le tableau.

Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton **Supprimer**. Pour modifier les paramètres d'une règle, sélectionnez la règle et cliquez sur le bouton **Modifier**, ou double-cliquez dessus. Effectuez les modifications souhaitées dans la fenêtre de configuration.

Pour ajouter manuellement une règle, cliquez sur le bouton **Ajouter** et configurer les paramètres de la règle dans la fenêtre de configuration.

19.4.1. Fenêtre de configuration

Lorsque vous modifiez ou ajoutez manuellement une règle, une fenêtre de configuration apparaît.


BitDefender Assistant Règle de cookie
Domaine :
Tous
Domaine :
Sélectionner une action
Autorisé
Refuser
Sélectionner la Direction
Sortant
Entrant
Tous les deux
Sélectionnez les sites web et les domaines dont vous voulez accepter ou refuser les cookies. Les cookies sont utilisés pour observer les habitudes de navigation et d'autres informations. Sachez toutefois que certains sites ne peuvent fonctionner correctement sans cookies.
Terminer
Annuler

Sélectionner l'Adresse, l'Action et la Direction

Vous pouvez définir les paramètres:

- **Adresse domaine** - vous pouvez introduire le domaine sur lequel porte la règle.
- **Action** - sélectionnez l'action de la règle.

Action	Description
Autoriser	Les cookies de ce domaine seront autorisés.
Interdire	Les cookies de ce domaine ne seront pas autorisés.

- **Direction** - sélectionner la direction du trafic.

Type	Description
Sortant	La règle s'applique seulement aux envois d'informations vers les serveurs accédés.
Entrant	La règle s'applique seulement aux envois d'informations en provenance des serveurs accédés.
Les deux	La règle s'applique dans les deux directions.

Note

Vous pouvez accepter des cookies et interdire leur envoi en sélectionnant l'action **Interdire** et la direction **Sortant**.

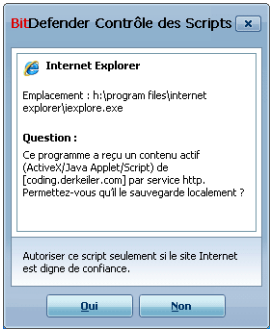
Cliquez sur **Terminer**.

19.5. Contrôle des scripts

Les Scripts et d'autres codes comme les contrôles ActiveX et Applets Java, qui sont utilisés pour créer des pages web interactives, peuvent être programmés pour avoir des effets néfastes. Les éléments ActiveX, par exemple, peuvent obtenir un accès total à vos données et peuvent lire des données depuis votre ordinateur, supprimer des informations, capturer des mots de passe et intercepter des messages lorsque vous êtes en ligne. Vous devriez accepter les contenus actifs uniquement sur les sites que vous connaissez et auxquels vous faites parfaitement confiance.

BitDefender vous laisse le choix d'exécuter ou de bloquer ces éléments.

Avec le **Contrôle de scripts** vous pourrez définir les sites web dans lesquels vous avez confiance ou non. BitDefender vous demandera votre permission dès qu'un site web essaiera d'activer un script ou tout type de contenu actif:

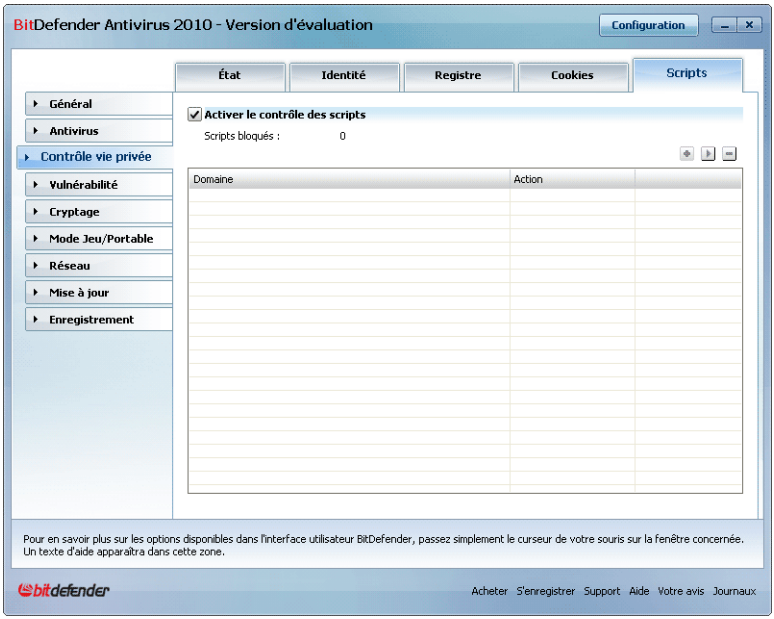

BitDefender Contrôle des Scripts
Internet Explorer
Emplacement : h:\program files\internet explorer\iexplore.exe
Question :
Ce programme a reçu un contenu actif (ActiveX/Java Applet/Script) de [coding.derkeiler.com] par service http. Permettez-vous qu'il le sauvegarde localement ?
Autoriser ce script seulement si le site Internet est digne de confiance.
Oui
Non

Alerte de scripts suspects

Vous pouvez voir le nom de la ressource.

Cliquez sur **Oui** ou sur **Non** et une règle sera créée, appliquée, et ajoutée au tableau des règles.

Pour configurer le contrôle des scripts, allez dans **Contrôle Vie privée>Script** en Mode Expert.



Contrôle des scripts

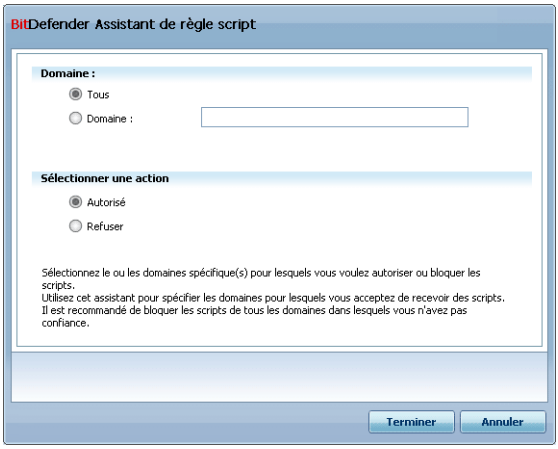
Vous pouvez voir les règles existantes dans le tableau.

Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton **Supprimer**. Pour modifier les paramètres d'une règle, sélectionnez la règle et cliquez sur le bouton **Modifier**, ou double-cliquez dessus. Effectuez les modifications souhaitées dans la fenêtre de configuration.

Pour créer manuellement une règle, cliquez sur le bouton **Ajouter** et configurer les paramètres de la règle dans la fenêtre de configuration.

19.5.1. Fenêtre de configuration

Lorsque vous modifiez ou ajoutez manuellement une règle, une fenêtre de configuration apparaît.


BitDefender Assistant de règle script
Domaine :
Tous
Domaine :
Sélectionner une action
Autorisé
Refuser
Sélectionnez le ou les domaines spécifique(s) pour lesquels vous voulez autoriser ou bloquer les scripts.
Utilisez cet assistant pour spécifier les domaines pour lesquels vous acceptez de recevoir des scripts.
Il est recommandé de bloquer les scripts de tous les domaines dans lesquels vous n'avez pas confiance.
Terminer
Annuler

Sélectionnez l'Adresse et l'Action

Vous pouvez définir les paramètres:

- **Adresse domaine** - vous pouvez introduire le domaine sur lequel porte la règle.
- **Action** - sélectionnez l’action de la règle.

Action	Description
Autoriser	Les scripts de ce domaine seront exécutés.
Interdire	Les scripts de ce domaine ne seront pas exécutés.

Cliquez sur **Terminer**.

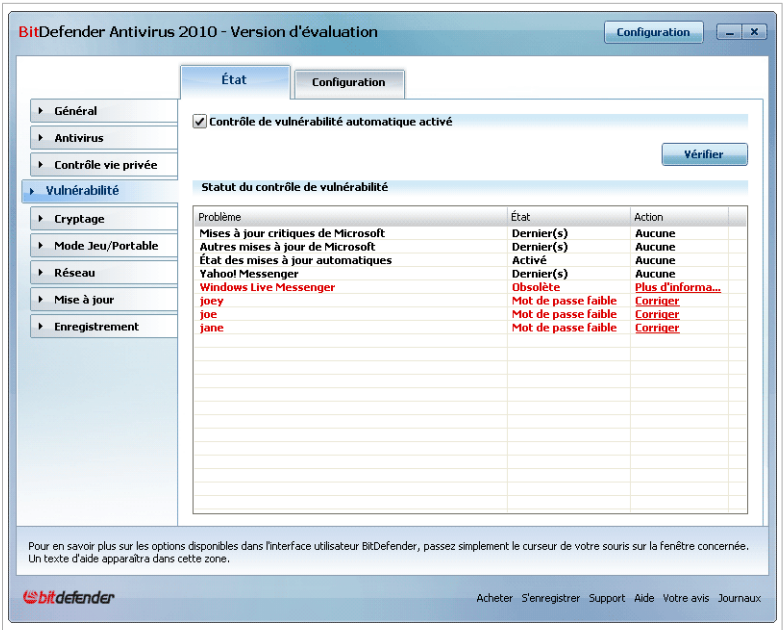
20. Vulnérabilité

Une étape importante permettant de préserver votre ordinateur contre les personnes malveillantes et les menaces est de maintenir à jour votre système d'exploitation et vos principales applications. De plus, afin de prévenir tout accès physique non autorisé à votre ordinateur, il est recommandé d'utiliser des mots de passe complexes (qui ne peuvent pas être devinés trop facilement) pour chaque compte utilisateur Windows.

BitDefender vérifie à intervalle régulier les vulnérabilités de votre système et vous informe des problèmes rencontrés.

20.1. État

Pour configurer la vérification automatique des vulnérabilités ou lancer un Contrôle de vulnérabilité, allez dans **Vulnerabilités> État** en Mode Expert.



État de la vulnérabilité

Le tableau affiche les problèmes traités lors du dernier contrôle de vulnérabilité ainsi que leur état. Vous pouvez consulter l'action à entreprendre pour réparer

chaque vulnérabilité, s'il y en a. Si l'action est **Aucune**, alors le problème en question ne représente pas une vulnérabilité.

Important
Pour être automatiquement averti en cas de vulnérabilités du système ou des applications, veuillez garder l'option **Vérification automatique des vulnérabilités** activée.

20.1.1. Réparation des vulnérabilités

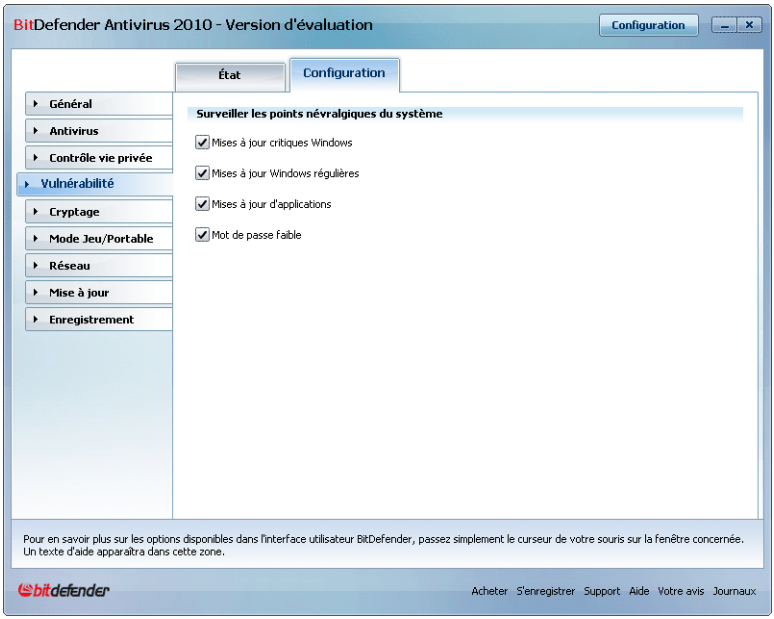
En fonction du problème, procédez comme suit pour corriger une vulnérabilité spécifique :

- Si les mises à jour Windows sont disponibles, cliquez sur **Installer** dans la colonne **Action** pour les installer.
- Si une application n'est pas à jour, cliquez sur le lien **Page d'accueil**fourni pour télécharger et installer la dernière version de cette application.
- Si un compte utilisateur Windows a un mot de passe vulnérable, cliquez sur **Corriger** pour obliger l'utilisateur à modifier son mot de passe lors de la prochaine connexion ou pour changer le mot de passe par vous-même. Pour avoir un mot de passe Fort, utilisez un mélange de lettres majuscules, minuscules, de nombres et de caractères spéciaux (comme par exemple #, $ ou @).

Pour rechercher des vulnérabilités sur votre ordinateur, cliquez sur **Vérifier maintenant** et suivez les instructions de l'assistant. Pour plus d'informations, reportez-vous à « *Assistant du Contrôle de Vulnérabilité* » (p. 67).

20.2. Configuration

Pour configurer les paramètres de la vérification automatique des vulnérabilités, allez dans **Vulnérabilités>Paramètres** en Mode Expert.


BitDefender Antivirus 2010 - Version d'évaluation
Configuration
État
Configuration
Général
Antivirus
Contrôle vie privée
Vulnérabilité
Cryptage
Mode Jeu/Portable
Réseau
Mise à jour
Enregistrement
Surveiller les points névralgiques du système
Mises à jour critiques Windows
Mises à jour Windows régulières
Mises à jour d'applications
Mot de passe faible
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

Paramètres de la vérification automatique des vulnérabilités.

Cochez les cases correspondantes aux vulnérabilités système que vous voulez analyser régulièrement :

- **Mises à jour Windows critiques**
- **Mises à jour Windows régulières**
- **Mises à jour d'applications**
- **Mots de passe vulnérables**

Note

Si vous décochez la case correspondant à une certaine vulnérabilité, BitDefender ne vous informera plus des problèmes la concernant.

21. Cryptage de messagerie instantanée

Par défaut, BitDefender crypte toutes vos sessions de messagerie instantanée, à condition que :

- votre correspondant ait installé sur son ordinateur une version de BitDefender qui prenne en charge le cryptage de messagerie instantanée et que ce dernier soit activé pour l'application de messagerie instantanée utilisée pour converser ;
- vous et votre correspondant utilisiez soit Yahoo Messenger, soit Windows Live (MSN) Messenger.

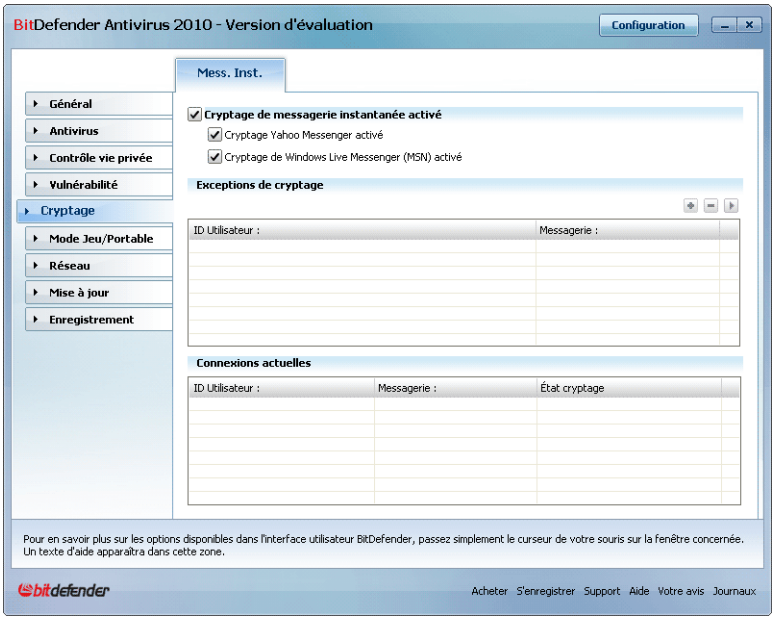
Important

BitDefender ne cryptera pas la conversation si le correspondant utilise une application à interface Web, telle que Meebo, ou si l'un des correspondants utilise Yahoo! et l'autre Windows Live (MSN).

Pour configurer le cryptage de messagerie instantanée, allez dans **Cryptage>Messagerie Instantanée** en Mode Expert.

Note

Vous pouvez aisément configurer le cryptage de messagerie instantanée en utilisant la barre d'outils BitDefender dans la fenêtre de chat. Pour plus d'informations, reportez-vous à « *Intégration dans les Programmes de Messagerie Instantanée* » (p. 210).



Cryptage de messagerie instantanée

Par défaut, le cryptage de messagerie instantanée est activé pour Yahoo Messenger et Windows Live (MSN) Messenger. Vous pouvez désactiver ce cryptage de messagerie instantanée soit entièrement, soit uniquement pour une application de chat spécifique.

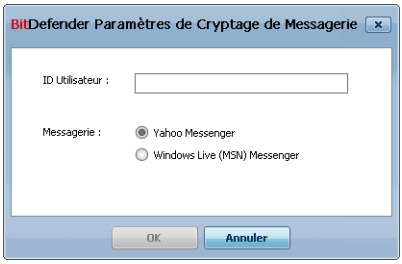
Deux tableaux sont affichés :

- **Exclusions de Cryptage** - Liste les contacts de messagerie et les messageries correspondantes pour lesquels le cryptage est désactivé. Pour effacer un contact de la liste, sélectionnez-le et cliquez sur le bouton **Effacer**.
- **Connexions actuelles** - Liste les connexions de messageries instantanées qui sont cryptées ou non. (Contacts et messageries associées) Une connexion peut ne pas être cryptée pour les raisons suivantes :
  - Vous avez volontairement désactivé le cryptage pour un contact particulier.
  - Votre contact n'a pas de version BitDefender installée supportant le cryptage des messageries instantanées.

21.1. Désactiver le cryptage pour des utilisateurs spécifiques

Pour désactiver le cryptage pour un utilisateur spécifique, suivez ces étapes :

1. Cliquez sur le bouton **Ajouter** pour ouvrir la fenêtre de configuration.



Ajout de contacts

2. Tapez dans le champ de saisie l'identifiant utilisateur de votre contact.
3. Sélectionnez l'application de messagerie instantanée associée au contact.
4. Cliquez sur **OK**.

22. Mode Jeu / Portable

Le module Réglages du produit vous permet de configurer les modes de fonctionnement spéciaux de BitDefender :

- Mode Jeu - modifie temporairement les paramètres du produit, de façon à minimiser la consommation de ressources lorsque vous jouez à un jeu vidéo.
- Mode Portable - évite l'exécution de tâches planifiées lorsque l'ordinateur portable est alimenté par sa batterie, afin de préserver l'autonomie de celle-ci.

22.1. Mode Jeu

Le Mode Jeu modifie temporairement les paramètres de protection afin de minimiser leur impact sur les performances du système. Les paramètres suivants sont appliqués lorsque vous êtes en Mode Jeu :

- Toutes les alertes et pop-ups BitDefender sont désactivées.
- Le niveau de la protection en temps réel de BitDefender est paramétré sur **Tolérant**.
- Les mises à jour sont désactivées par défaut.

Note

Pour modifier ce paramètre, rendez-vous dans Mise à jour>Paramètres et décochez la case **Ne pas mettre à jour si le Mode Jeu est actif**.

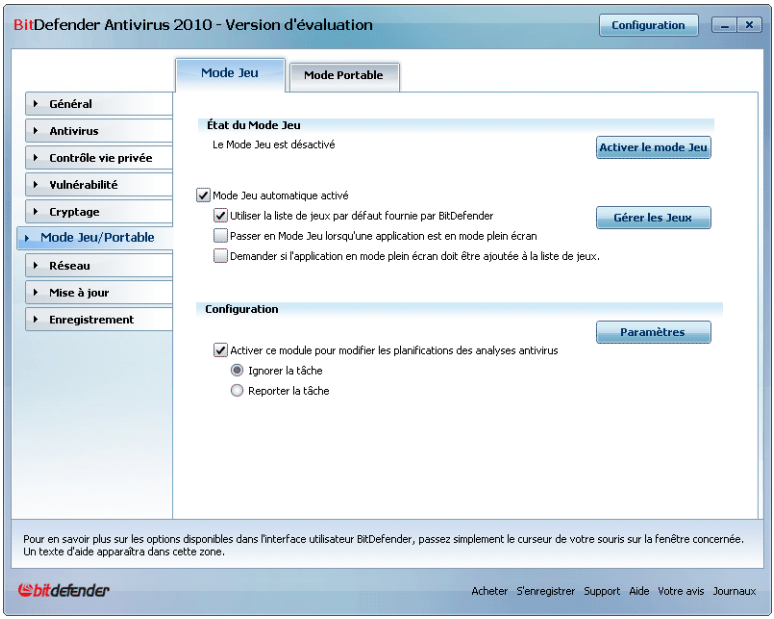
- Les tâches d'analyse planifiées sont désactivées par défaut.

Par défaut, BitDefender passe automatiquement en Mode Jeu lorsque vous lancez un jeu figurant dans la liste des jeux connus de BitDefender, ou lorsqu'une application s'exécute en mode plein écran. Vous pouvez passer manuellement en Mode Jeu en utilisant le raccourci clavier par défaut `Ctrl+Alt+Shift+G`. Nous vous recommandons fortement de quitter le Mode Jeu lorsque vous avez fini de jouer (vous pouvez pour ce faire utiliser le même raccourci clavier par défaut `Ctrl+Alt+Shift+G`).

Note

Lorsque vous êtes en Mode Jeu, vous pouvez voir la lettre G incrustée sur l'icône BitDefender.

Pour configurer le Mode Jeu, allez dans **Mode Jeu/Portable> Mode Jeu** en Mode Expert.


BitDefender Antivirus 2010 - Version d'évaluation
Configuration
Mode Jeu
Mode Portable
Général
Antivirus
Contrôle vie privée
Vulnérabilité
Cryptage
Mode Jeu/Portable
Réseau
Mise à jour
Enregistrement
État du Mode Jeu
Le Mode Jeu est désactivé
Activer le mode Jeu
Mode Jeu automatique activé
Utiliser la liste de jeux par défaut fournie par BitDefender
Gérer les Jeux
Passer en Mode Jeu lorsqu'une application est en mode plein écran
Demander si l'application en mode plein écran doit être ajoutée à la liste de jeux.
Configuration
Paramètres
Activer ce module pour modifier les planifications des analyses antivirus
Ignorer la tâche
Reporter la tâche
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée.
Un texte d'aide apparaîtra dans cette zone.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

Mode Jeu

Vous pouvez vérifier l'état du Mode Jeu dans la partie supérieure de la section. Vous pouvez cliquer sur **Activer le Mode Jeu** ou **Désactiver le Mode Jeu** pour modifier l'état en cours.

22.1.1. Configuration du Mode Jeu automatique

Le Mode Jeu automatique permet à BitDefender de passer automatiquement en Mode Jeu lorsque l'exécution d'un jeu est détectée. Voici les options d'analyse que vous pouvez configurer :

- **Utiliser la liste de jeux par défaut fournie par BitDefender** - permet de passer automatiquement en Mode Jeu lorsque vous lancez un jeu figurant dans la liste de jeux connus de BitDefender. Pour afficher cette liste, cliquez sur **Gérer les Jeux** puis sur **Liste des Jeux**.
- **Passer en Mode Jeu lorsqu'une application est en mode plein écran** - permet de passer automatiquement en Mode Jeu lorsqu'une application s'exécute en mode plein écran.
- **Ajouter l'application à la liste de jeux ?** - permet d'être notifié pour l'ajout d'une nouvelle application à la liste de jeux, à la fermeture du mode plein écran.

Si vous ajoutez une nouvelle application à la liste de jeux, la prochaine fois que vous lancerez celle-ci, BitDefender passera automatiquement en Mode Jeu.

Note
Si vous ne voulez pas que BitDefender passe automatiquement en Mode Jeu, décochez la case **Mode Jeu automatique**.

22.1.2. Gestion de la liste de jeux

BitDefender passe automatiquement en Mode Jeu lorsque vous lancez une application figurant dans la liste de jeux. Pour consulter et gérer la liste de jeux, cliquez sur **Gérer les jeux**. Une nouvelle fenêtre s'affiche.

BitDefender Gérer les Jeux
Ma Liste de Jeux
Nom
Liste des Jeux
Ceci est la liste des jeux que vous avez définis qui feront automatiquement passer BitDefender en Mode Jeu.
OK

Liste de jeux

De nouvelles applications sont automatiquement ajoutées à la liste dans les situations suivantes :

- Vous lancez un jeu figurant dans la liste de jeux connus de BitDefender. Pour afficher cette liste, cliquez sur **Liste des Jeux**.
- Lors de la fermeture du mode plein écran, vous ajoutez l'application à la liste de jeux à partir de la fenêtre d'invite.

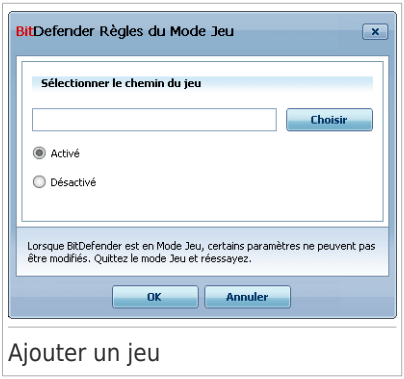
Si vous voulez désactiver le Mode Jeu automatique pour une application spécifique de la liste, décochez la case correspondante. Vous avez tout intérêt à désactiver le Mode Jeu automatique pour les applications standard qui utilisent le mode plein écran, telles que les navigateurs Web et les lecteurs vidéo.

Pour gérer la liste de jeux, vous pouvez utiliser les boutons disposés en haut du tableau :

- **Ajouter** - ajoute une nouvelle application à la liste de jeux.
- **Supprimer** - supprime une application de la liste des jeux.
- **Éditer** - permet de modifier une entrée existante dans la liste de jeux.

Ajout ou édition de jeux

Lorsque vous ajoutez ou éditez une entrée de la liste de jeux, la fenêtre suivante apparaît :


BitDefender Règles du Mode Jeu
Sélectionner le chemin du jeu
Choisir
Activé
Désactivé
Lorsque BitDefender est en Mode Jeu, certains paramètres ne peuvent pas être modifiés. Quittez le mode Jeu et réessayez.
OK
Annuler

Ajouter un jeu

Cliquez sur **Parcourir** pour sélectionner l'application, ou tapez le chemin d'accès complet à l'application dans le champ de saisie.

Si vous ne voulez pas passer automatiquement en Mode Jeu lorsque l'application sélectionnée s'exécute, sélectionnez **Désactiver**.

Cliquez sur **OK** pour ajouter l'entrée à la liste de jeux.

22.1.3. Configuration des paramètres du Mode Jeu

Utilisez ces options pour configurer le comportement avec des tâches planifiées :

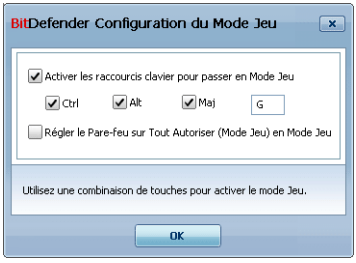
- **Activer ce module pour modifier les planifications d'analyses antivirus** - permet d'éviter l'exécution d'analyses antivirus planifiées lorsque le Mode Jeu est activé. Vous pouvez choisir une des options suivantes :

Option	Description
Ignorer la tâche	Annule complètement l'exécution de la tâche planifiée.
Reporter la tâche	Exécute la tâche planifiée juste après la désactivation du Mode Jeu.

22.1.4. Changer le raccoruci clavier du Mode Jeu

Vous pouvez passer manuellement en Mode Jeu en utilisant le raccourci clavier par défaut `Ctrl+Alt+Shift+G`. Pour changer le raccourci clavier, suivez ces étapes :

1. Cliquez sur **Paramètres avancés**. Une nouvelle fenêtre s'affiche.


BitDefender Configuration du Mode Jeu
Activer les raccourcis clavier pour passer en Mode Jeu
Ctrl
Alt
Maj
G
Régler le Pare-feu sur Tout Autoriser (Mode Jeu) en Mode Jeu
Utilisez une combinaison de touches pour activer le mode Jeu.
OK

Paramètres

2. Sous l'option **Utiliser le raccourci**, définissez le raccourci clavier désiré :
   - Choisissez la touche que vous souhaitez utiliser en cochant l'une des suivantes : touche Contrôle (`Ctrl`), Touche Shift(`Shift`) ou touche Alt (`Alt`).
   - Dans le champ éditable, entrez la lettre que vous souhaitez utiliser.

   Par exemple, si vous souhaitez utiliser le raccourci `Ctrl+Alt+D`, vous devez cocher seulement `Ctrl` et `Alt` et tapez `D`.

   Note
   En décochant la case **Utiliser le raccourci**, vous désactivez le raccourci clavier.

3. Cliquez **OK** pour sauvegarder les changements.

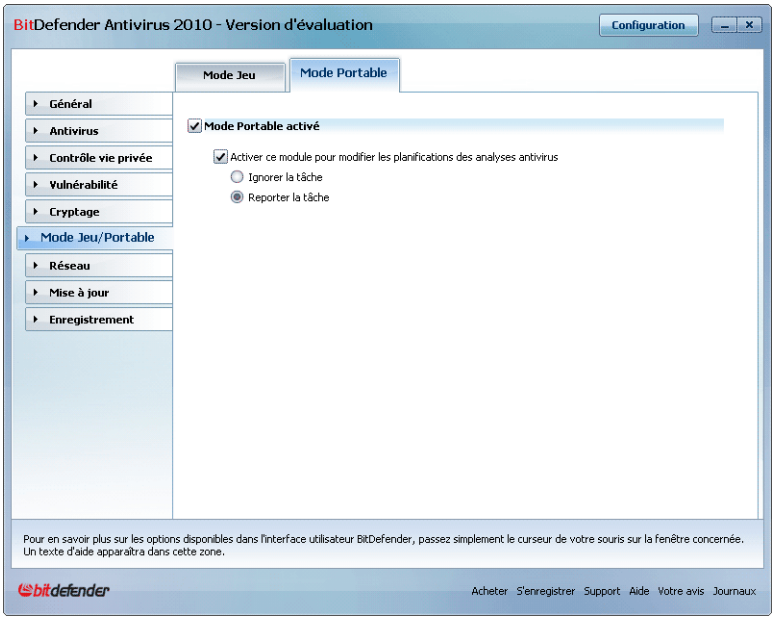
22.2. Mode Portable

Le Mode Portable est spécialement conçu pour les utilisateurs d'ordinateurs portables et de notebooks. Son objectif est de minimiser l'impact de BitDefender sur la consommation d'énergie lorsque ces périphériques sont alimentés par leur batterie.

En Mode Portable, les tâches planifiées sont désactivées par défaut.

BitDefender détecte le passage d'une alimentation secteur à une alimentation sur batterie et passe automatiquement en Mode Portable. De la même manière, BitDefender quitte automatiquement le Mode Portable lorsqu'il détecte que l'ordinateur portable ne fonctionne plus sur batterie.

Pour configurer le Mode Portable, allez dans **Mode Jeu/Portable> Mode Portable** en Mode Expert.


BitDefender Antivirus 2010 - Version d'évaluation
Configuration
Mode Jeu
Mode Portable
Général
Antivirus
Contrôle vie privée
Vulnérabilité
Cryptage
Mode Jeu/Portable
Réseau
Mise à jour
Enregistrement
Mode Portable activé
Activer ce module pour modifier les planifications des analyses antivirus
Ignorer la tâche
Reporter la tâche
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

Mode Portable

Vous pouvez vérifier si le Mode Portable est activé ou désactivé. Si le Mode Portable est activé, BitDefender applique les paramètres configurés lorsque l'ordinateur portable fonctionne sur batterie.

22.2.1. Configuration des paramètres du Mode Portable

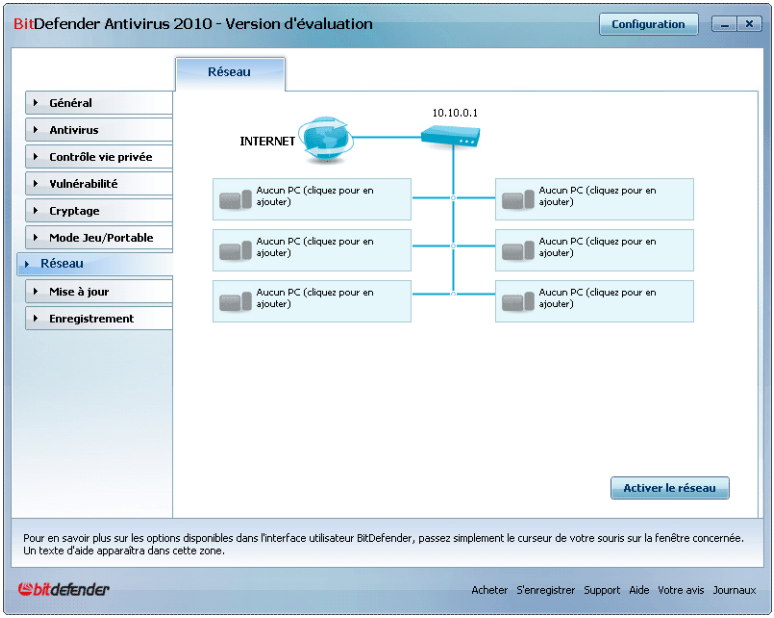
Utilisez ces options pour configurer le comportement avec des tâches planifiées :

- **Activer ce module pour modifier les planifications d'analyses antivirus** - permet d'éviter l'exécution d'analyses planifiées lorsque le Mode Portable est activé. Vous pouvez choisir une des options suivantes :

Option	Description
Ignorer la tâche	Annule complètement l'exécution de la tâche planifiée.
Reporter la tâche	Exécuter la tâche planifiée lorsque vous quitterez le Mode Portable.

23. Réseau Domestique

Le module Réseau vous permet de gérer les produits BitDefender installés sur tous les ordinateurs de votre foyer à partir d'un seul et même ordinateur.



Carte réseau

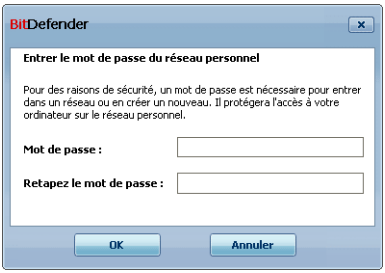
Vous devez suivre ces étapes pour pouvoir gérer les produits BitDefender installés sur tous les ordinateurs de votre foyer :

1. Rejoindre le réseau domestique BitDefender via votre ordinateur. Rejoindre le réseau consiste à configurer un mot de passe d'administration pour la gestion du réseau domestique.
2. Allumez chaque ordinateur que vous voulez gérer et rejoignez le réseau à partir de ceux-ci (en saisissant le mot de passe).
3. Revenez sur votre ordinateur et ajoutez les ordinateurs que vous voulez gérer.

23.1. Rejoindre le réseau BitDefender

Procédez comme suit pour rejoindre le réseau domestique BitDefender :

1. Cliquez sur **Activer le Réseau**. Vous serez invité à définir le mot de passe de gestion de réseau domestique.


BitDefender
Entrer le mot de passe du réseau personnel
Pour des raisons de sécurité, un mot de passe est nécessaire pour entrer dans un réseau ou en créer un nouveau. Il protégera l'accès à votre ordinateur sur le réseau personnel.
Mot de passe :
Retapez le mot de passe :
OK
Annuler

Définir le mot de passe

2. Entrez le même mot de passe dans chacun des champs de saisie.
3. Cliquez sur **OK**.

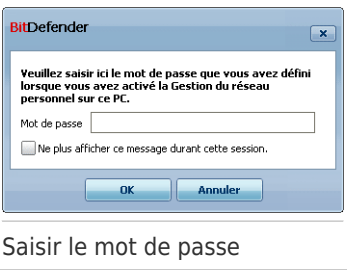
Vous pouvez voir apparaître le nom de l'ordinateur sur la carte réseau.

23.2. Ajout d'ordinateurs au réseau BitDefender

Avant de pouvoir ajouter un ordinateur au réseau domestique BitDefender, vous devez définir le mot de passe de gestion de réseau domestique BitDefender sur l'ordinateur à ajouter.

Procédez comme suit pour ajouter un ordinateur au réseau domestique BitDefender :

1. Cliquez sur **Ajouter un PC**. Vous serez invité à saisir le mot de passe local de gestion de réseau domestique.


BitDefender
Veuillez saisir ici le mot de passe que vous avez défini lorsque vous avez activé la Gestion du réseau personnel sur ce PC.
Mot de passe
Ne plus afficher ce message durant cette session.
OK
Annuler

Saisir le mot de passe

2. Tapez le mot de passe de gestion de réseau domestique et cliquez sur **OK**. Une nouvelle fenêtre s'affiche.

Ajouter un PC

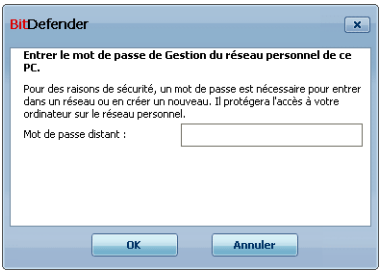
Vous pouvez voir à l'écran la liste des ordinateurs rattachés au réseau. La signification des icônes est la suivante :

Indique un ordinateur en ligne sans aucun produit BitDefender installé.

Indique un ordinateur en ligne avec BitDefender installé.

Indique un ordinateur hors connexion avec BitDefender installé.

3. Choisissez une des possibilités suivantes :
   - Sélectionnez dans la liste le nom de l'ordinateur à ajouter.
   - Tapez l'adresse IP ou le nom de l'ordinateur à ajouter dans le champ correspondant.
4. Cliquez sur **Ajouter**. Vous serez invité à saisir le mot de passe de gestion de réseau domestique de l'ordinateur concerné.


BitDefender
Entrer le mot de passe de Gestion du réseau personnel de ce PC.
Pour des raisons de sécurité, un mot de passe est nécessaire pour entrer dans un réseau ou en créer un nouveau. Il protégera l'accès à votre ordinateur sur le réseau personnel.
Mot de passe distant :
OK
Annuler

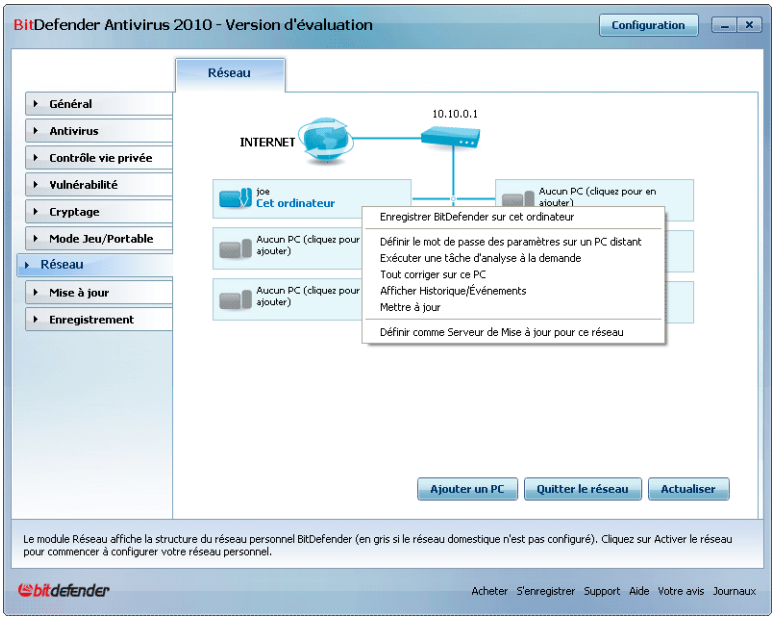
Authentification

5. Tapez le mot de passe de gestion de réseau domestique défini sur l'ordinateur concerné.
6. Cliquez sur **OK**. Si vous avez spécifié le bon mot de passe, le nom de l'ordinateur sélectionné apparaît sur la carte réseau.

Note
Vous pouvez ajouter jusqu'à cinq ordinateurs sur la carte réseau.

23.3. Gestion du réseau BitDefender

Une fois votre réseau domestique BitDefender créé, vous pouvez gérer l'ensemble des produits BitDefender à partir d'un seul et même ordinateur.


BitDefender Antivirus 2010 - Version d'évaluation
Configuration
Réseau
Général
Antivirus
Contrôle vie privée
Vulnérabilité
Cryptage
Mode Jeu/Portable
Réseau
Mise à jour
Enregistrement
INTERNET
10.10.0.1
joe
Cet ordinateur
Aucun PC (cliquez pour en ajouter)
Aucun PC (cliquez pour ajouter)
Aucun PC (cliquez pour ajouter)
Enregistrer BitDefender sur cet ordinateur
Définir le mot de passe des paramètres sur un PC distant
Exécuter une tâche d'analyse à la demande
Tout corriger sur ce PC
Afficher Historique/Événements
Mettre à jour
Définir comme Serveur de Mise à jour pour ce réseau
Ajouter un PC
Quitter le réseau
Actualiser
Le module Réseau affiche la structure du réseau personnel BitDefender (en gris si le réseau domestique n'est pas configuré). Cliquez sur Activer le réseau pour commencer à configurer votre réseau personnel.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

Carte réseau

Si vous déplacez le curseur sur un ordinateur de la carte réseau, vous pouvez consulter quelques informations le concernant (nom, adresse IP, nombre de problèmes affectant la sécurité du système, état d'enregistrement de BitDefender).

En cliquant sur le nom d'un ordinateur sur la carte du réseau, vous pouvez voir toutes les tâches administratives que vous pouvez lancer sur cet ordinateur distant.

- **Retirer le PC du réseau personnel**

  Vous permet de retirer un PC du réseau.

- **Enregistrer BitDefender sur cet ordinateur**

  Vous permet d'enregistrer BitDefender sur cet ordinateur en entrant une clé de licence.

- **Définir un mot de passe des paramètres sur un PC distant**

  Vous permet de créer un mot de passe pour limiter l'accès aux paramètres de BitDefender sur ce PC.

- **Lancer une tâche d'analyse à la demande**

Vous permet de lancer une analyse à la demande sur un ordinateur distant. Vous pouvez réaliser l'une des tâches d'analyse suivantes : Analyse de Mes Documents, Analyse du Système ou Analyse Approfondie du Système.

- **Corriger tous les problèmes de ce PC**

  Vous permet de corriger les problèmes qui affectent la sécurité de cet ordinateur à l'aide de l'assistant Tout corriger.

- **Afficher Historique/Événements**

  Vous permet d'accéder au module **Historique&Événements** du produit BitDefender installé sur cet ordinateur.

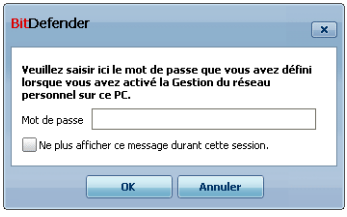
- **Mettre à jour**

  Lance le processus de Mise à jour du produit BitDefender installé sur cet ordinateur.

- **Définir comme Serveur de Mise à Jour pour ce réseau**

  Vous permet de définir cet ordinateur comme serveur de mise à jour pour tous les produits BitDefender installés sur les ordinateurs de ce réseau. Utiliser cette option réduira le trafic Internet car seul un ordinateur du réseau se connectera à Internet pour télécharger des mises à jour.

Avant de lancer une tâche sur un ordinateur spécifique, vous serez invité à saisir le mot de passe local de gestion de réseau domestique.


BitDefender
Veuillez saisir ici le mot de passe que vous avez défini lorsque vous avez activé la Gestion du réseau personnel sur ce PC.
Mot de passe
Ne plus afficher ce message durant cette session.
OK
Annuler

Saisir le mot de passe

Tapez le mot de passe de gestion de réseau domestique et cliquez sur **OK**.

Note

Si vous prévoyez de lancer plusieurs tâches, il peut s'avérer utile de sélectionner l'option **Ne plus afficher ce message durant cette session**. En sélectionnant cette option, vous n'aurez plus à saisir le mot de passe pour la session en cours.

24. Mise à jour

Chaque jour, de nouveaux codes malveillants sont détectés et identifiés. C'est pourquoi il est très important que BitDefender soit à jour dans les signatures de codes malveillants.

Si vous êtes connecté à Internet par câble ou DSL, BitDefender s'en occupera automatiquement. Il lance la procédure de mise à jour de la base virale à chaque fois que vous démarrez votre ordinateur puis toutes les **heures**.

Si une mise à jour a été trouvée, elle sera installée automatiquement ou il vous sera demandé de confirmer son installation, selon les paramètres de mise à jour automatique.

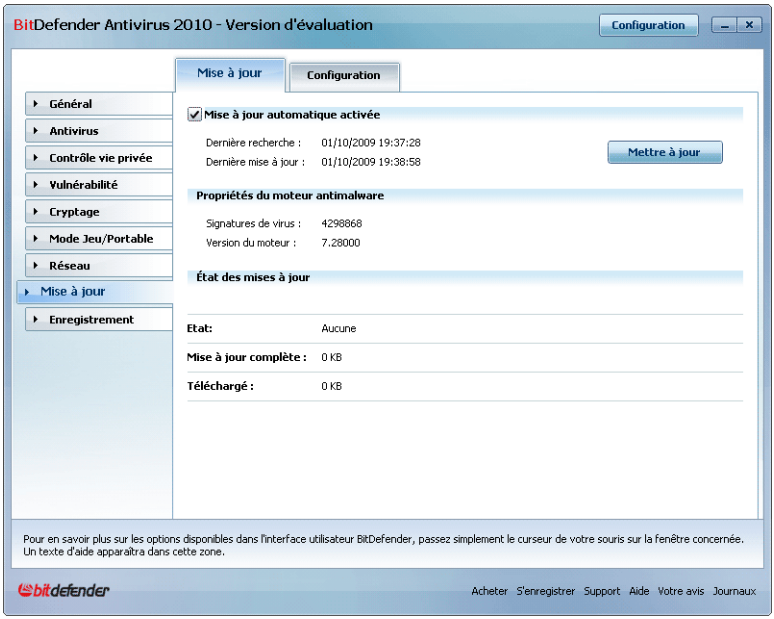
Le processus de mise à jour est exécuté à la volée, ce qui signifie que les fichiers nécessitant une mise à jour sont remplacés progressivement. Ainsi, le processus de mise à jour n'affecte pas le fonctionnement du produit tout en excluant tout problème de vulnérabilité en matière de sécurité.

La section Mise à jour de ce Manuel d'utilisation contient les thèmes suivants:

- **Mise à jour des moteurs antivirus** - comme de nouvelles menaces apparaissent, les fichiers contenant les signatures de virus doivent être mis à jour en permanence contre elles. Elles s'affichent sous le nom de **Virus Definitions Update**.
- **Mise à jour des moteurs antispyware** - de nouvelles signatures seront ajoutées à la base de données. Elles s'affichent sous le nom de **Spyware Definitions Update**.
- **Mise à jour produit** - lorsqu'une nouvelle version du produit est prête, de nouvelles fonctions et techniques d'analyse sont introduites afin d'augmenter les performances du produit. Ces mises à jour sont affichées sous le nom de **Product Update**.

24.1. Mise à jour automatique

Pour consulter des informations relatives aux mises à jour et exécuter des mises à jour automatiques, allez dans **Mise à jour>Mise à jour** en Mode Expert.


BitDefender Antivirus 2010 - Version d'évaluation
Configuration
Mise à jour
Configuration
Général
Antivirus
Contrôle vie privée
Vulnérabilité
Cryptage
Mode Jeu/Portable
Réseau
Mise à jour
Enregistrement
Mise à jour automatique activée
Dernière recherche : 01/10/2009 19:37:28
Dernière mise à jour : 01/10/2009 19:38:58
Mettre à jour
Propriétés du moteur antimalware
Signatures de virus : 4298868
Version du moteur : 7.28000
État des mises à jour
Etat: Aucune
Mise à jour complète : 0 KB
Téléchargé : 0 KB
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

Mise à jour automatique

C'est ici que vous pouvez consulter la date de la dernière recherche de mises à jour et celle de la dernière mise à jour, ainsi que des informations sur la dernière mise à jour effectuée (ou les erreurs rencontrées). Sont également affichées des informations sur la version actuelle du moteur de recherche et le nombre de signatures.

Si vous ouvrez cette section pendant une mise à jour, vous pourrez accéder à l'état du téléchargement.

Important

Pour être protégé contre les dernières menaces, il est impératif de laisser la **mise à jour automatique** active.

24.1.1. Demandes de mise à jour

La mise à jour automatique peut aussi etre effectuée n'importe quand en cliquant sur **Mettre à jour**. Cette mise à jour est connue aussi sous l'appellation **Mettre à jour a la demande de l'utilisateur**.

Le module **Mise à jour**se connecte au serveur de mise à jour BitDefender et recherche les mises à jour disponibles. Si une mise à jour est détectée, vous serez

invité à la confirmer ou elle sera effectuée automatiquement en fonction des options que vous aurez définies dans la section Paramètres de la mise à jour manuelle.

Important
Il peut être nécessaire de redémarrer votre PC lorsque vous avez terminé une mise à jour. Nous vous recommandons de le faire dès que possible.

Note
Si vous êtes connecté à Internet via une connexion RTC (ou RNIS), nous vous conseillons de prendre l'habitude d'utiliser régulièrement les mises à jour à la demande.

24.1.2. Désactiver la mise à jour automatique

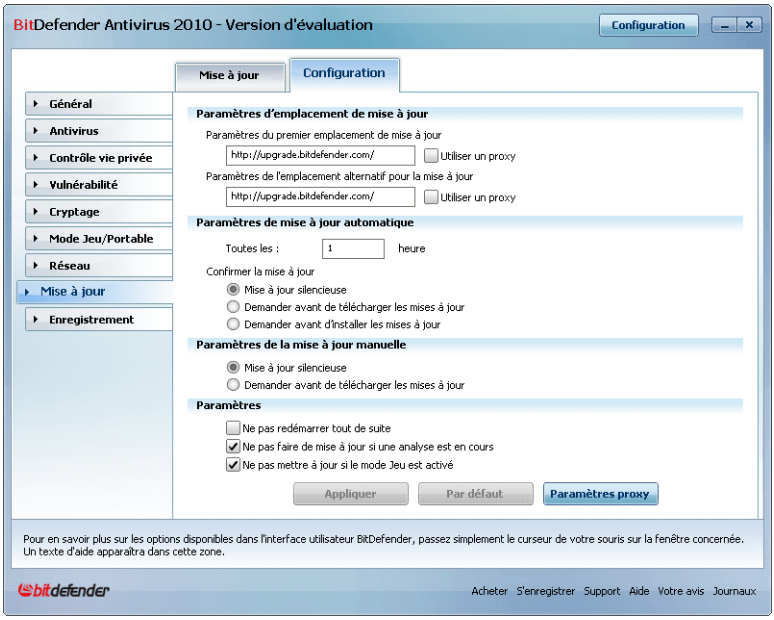
Si vous tentez de désactiver la mise à jour automatique, une fenêtre d'avertissement apparaît. Vous devez confirmer votre choix en sélectionnant dans le menu la durée pendant laquelle vous souhaitez désactiver la mise à jour automatique. Vous pouvez désactiver la mise à jour automatique pendant 5, 15 ou 30 minutes, 1 heure, en permanence ou jusqu'au redémarrage du système.

Avertissement
Cela peut poser un problème de sécurité important. Nous vous recommandons de désactiver la mise à jour automatique pendant le moins de temps possible. Si BitDefender n'est pas régulièrement mis à jour, il ne pourra pas vous protéger contre les dernières menaces.

24.2. Paramètres de mise à jour

Les mises à jour peuvent être réalisées depuis le réseau local, depuis Internet, directement ou à travers un serveur proxy. Par défaut, BitDefender recherche les mises à jour chaque heure sur Internet et installe celles qui sont disponibles sans vous en avertir.

Pour configurer les paramètres de mise à jour et gérer les serveurs proxy, allez dans **Mise à jour > Paramètres** en Mode Expert.


BitDefender Antivirus 2010 - Version d'évaluation
Configuration
Mise à jour
Configuration
Général
Antivirus
Contrôle vie privée
Vulnérabilité
Cryptage
Mode Jeu/Portable
Réseau
Mise à jour
Enregistrement
Paramètres d'emplacement de mise à jour
Paramètres du premier emplacement de mise à jour
http://upgrade.bitdefender.com/
Utiliser un proxy
Paramètres de l'emplacement alternatif pour la mise à jour
http://upgrade.bitdefender.com/
Utiliser un proxy
Paramètres de mise à jour automatique
Toutes les :
1
heure
Confirmer la mise à jour
Mise à jour silencieuse
Demander avant de télécharger les mises à jour
Demander avant d'installer les mises à jour
Paramètres de la mise à jour manuelle
Mise à jour silencieuse
Demander avant de télécharger les mises à jour
Paramètres
Ne pas redémarrer tout de suite
Ne pas faire de mise à jour si une analyse est en cours
Ne pas mettre à jour si le mode Jeu est activé
Appliquer
Par défaut
Paramètres proxy
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

Paramètres de mise à jour

Les paramètres de mise à jour sont regroupés en quatre catégories (**Paramètres d'emplacement de mise à jour**, **Paramètres de mise à jour automatique**, **Paramètres de mise à jour manuelle** et **Paramètres avancés**). Chaque catégorie est décrite séparément.

24.2.1. Paramétrage des emplacements de mise à jour

Pour configurer les emplacements de mise à jour, utilisez les options de la catégorie **Paramètres d'emplacement de mise à jour**.

Note
Ne configurez ces paramètres que si vous êtes connecté à un réseau local qui stocke les signatures de codes malveillants BitDefender localement ou si vous êtes connecté à Internet via un serveur proxy.

Pour effectuer des mises à jour plus fiables et plus rapides, vous pouvez configurer deux emplacements de mise à jour: un **premier emplacement de mise à jour** et un **emplacement alternatif de mise à jour** . Par défaut, ces emplacements sont identiques: `http://upgrade.bitdefender.com`.

Pour modifier l'un des emplacements de mise à jour, indiquez l'URL du site miroir local dans le champ **URL** correspondant à l'emplacement que vous souhaitez modifier.

Note

Nous vous recommandons de configurer le miroir local en tant qu'emplacement primaire, et de conserver l'emplacement secondaire inchangé, par mesure de sécurité, au cas où le miroir local deviendrait indisponible.

Si votre entreprise utilise un serveur proxy pour se connecter à Internet, cochez la case **Utiliser un proxy**, puis cliquez sur **Paramètres Proxy** pour configurer les paramètres du proxy. Pour plus d'informations, reportez-vous à « *Gestion des serveurs proxy* » (p. 196)

24.2.2. Configuration de la mise à jour automatique

Pour configurer le processus de mise à jour exécuté automatiquement par BitDefender, utilisez les options de la catégorie **Paramètres de mise à jour automatique**.

Vous pouvez spécifier le nombre d'heures entre deux recherches consécutives de mises à jour dans le champ **Mettre à jour tous/toutes les**. Par défaut, l'intervalle est d'une heure.

Pour déterminer comment le processus de mise à jour automatique doit être exécuté, sélectionnez l'une des options suivantes :

- **Mise à jour silencieuse** - BitDefender télécharge et implémente automatiquement la mise à jour.
- **Demander avant de télécharger les mises à jour** - chaque fois qu'une mise à jour est disponible, le système demande votre autorisation avant de la télécharger.
- **Demander avant d'installer les mises à jour** - chaque fois qu'une mise à jour est téléchargée, le système demande votre autorisation avant de l'installer.

24.2.3. Configuration de la mise à jour manuelle

Pour déterminer comment la mise à jour manuelle (mise à jour à la demande de l'utilisateur) doit être exécutée, sélectionnez l'une des options suivantes dans la catégorie **Paramètres de la mise à jour manuelle**:

- **Mise à jour silencieuse** - la mise à jour manuelle est exécutée automatiquement en tâche de fond, sans l'intervention de l'utilisateur.
- **Demander avant de télécharger les mises à jour** - chaque fois qu'une mise à jour est disponible, le système demande votre autorisation avant de la télécharger.

24.2.4. Configuration des paramètres avancés

Pour éviter que les mises à jour de BitDefender n'interfèrent avec votre travail, configurez les options au niveau des **Paramètres avancés**:

- **Attendre le redémarrage, au lieu de le demander à l'utilisateur** - Si une mise à jour nécessite un redémarrage, le produit continuera à utiliser les anciens fichiers jusqu'à la réinitialisation du système. L'utilisateur ne sera pas averti qu'il doit redémarrer et ne sera donc pas perturbé dans son travail par la mise à jour de BitDefender.
- **Ne pas faire la mise-à-jour si l'analyse est en déroulement** - BitDefender ne se mettra pas à jour si une analyse est en cours afin de ne pas perturber ce processus.

  Note
  Si une mise à jour de BitDefender a lieu pendant l'analyse, celle-ci sera interrompue.

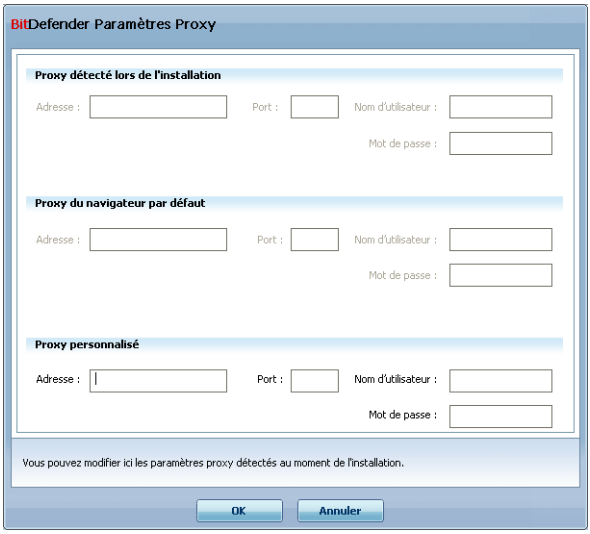
- **Ne pas mettre à jour si le mode jeu est actif** - BitDefender n'effectuera pas de mise à jour si le mode jeu est activé. Ainsi, vous limitez l'influence du produit sur les performances du système lorsque vous jouez.

24.2.5. Gestion des serveurs proxy

Si votre entreprise utilise un serveur proxy pour se connecter à Internet, vous devez spécifier les paramètres du proxy afin que BitDefender puisse se mettre à jour. Sinon, BitDefender utilisera les paramètres du proxy de l'administrateur qui a installé le produit ou du navigateur par défaut de l'utilisateur actuel, le cas échéant.

Note
Les paramètres du proxy peuvent être configurés uniquement par les utilisateurs possédant des droits d'administrateur ou par des utilisateurs privilégié (des utilisateurs qui connaissent le mot de passe pour accéder aux paramètres du produit).

Pour gérer les paramètres proxy, cliquez sur **Paramètres Proxy**. Une nouvelle fenêtre s'affichera.



Gestionnaire de proxy

Il existe trois catégories de paramètres de proxy:

- **Proxy détecté lors de l'installation** - Paramètres de configuration du proxy détectés pendant l'installation avec le compte Administrateur ; ces paramètres peuvent être modifiés uniquement si vous êtes connecté(e) avec ce compte. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, vous devez les indiquer dans les champs correspondants.
- **Proxy du Navigateur par défaut** - paramètres proxy de l'utilisateur acteur, extraits du navigateur par défaut. Si le serveur proxy requiert un nom d'utilisateur et un mot de passe, vous devez les spécifier dans les champs correspondants.

  Note
  Les navigateurs Web pris en charge sont Internet Explorer, Mozilla Firefox et Opera. Si vous utilisez un autre navigateur par défaut, BitDefender ne pourra pas obtenir les paramètres du proxy de l'utilisateur actuel.

- **Proxy Personnalisé** - paramètres proxy que vous pouvez configurer si vous êtes connecté(e) en tant qu'administrateur.

  Voici les paramètres à spécifier:
  - **Adresse** - saisissez l'IP du serveur proxy.
  - **Port** - saisissez le port utilisé par BitDefender pour se connecter au serveur proxy.
  - **Nom d'utilisateur** - entrez le nom d'utilisateur reconnu par le serveur proxy.

- **Mot de passe** - saisissez le mot de passe valide de l'utilisateur dont le nom vient d'être indiqué.

Lors de la tentative de connexion à Internet, chaque catégorie de paramètres de proxy est testée, jusqu'à ce que BitDefender parvienne à se connecter.

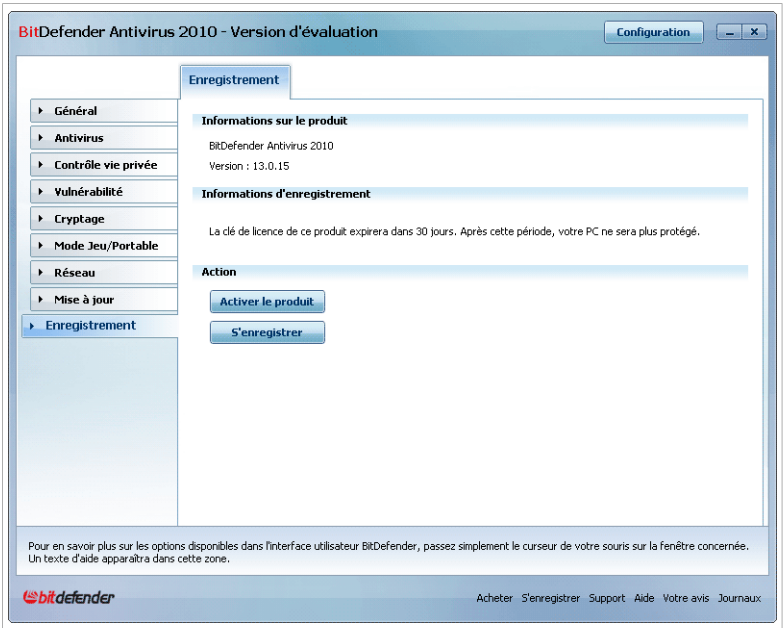
Tout d'abord, la catégorie contenant vos propres paramètres de proxy est utilisée pour la connexion Internet. Si elle ne fonctionne pas, ce sont alors les paramètres de proxy détectés lors de l'installation qui sont utilisés. Finalement, s'ils ne fonctionnent pas non plus, les paramètres du proxy de l'utilisateur actuel sont pris sur le navigateur par défaut et utilisés pour la connexion Internet.

Cliquez sur **OK** pour sauvegarder les modifications et fermez la fenêtre.

Cliquez sur **Appliquer** pour enregistrer les modifications ou cliquez sur **Défaut** pour charger les paramètres par défaut.

25. Enregistrement

Pour avoir accès à des informations complètes sur votre produit BitDefender et votre enregistrement, allez dans **Enregistrement** dans l'interface Expert.


BitDefender Antivirus 2010 - Version d'évaluation
Configuration
Enregistrement
Général
Antivirus
Contrôle vie privée
Vulnérabilité
Cryptage
Mode Jeu/Portable
Réseau
Mise à jour
Enregistrement
Informations sur le produit
BitDefender Antivirus 2010
Version : 13.0.15
Informations d'enregistrement
La clé de licence de ce produit expirera dans 30 jours. Après cette période, votre PC ne sera plus protégé.
Action
Activer le produit
S'enregistrer
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
bitdefender
Acheter S'enregistrer Support Aide Votre avis Journaux

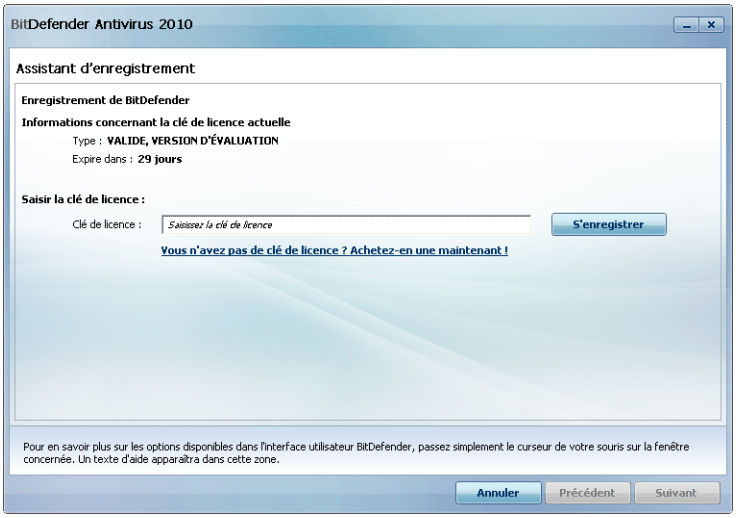
Enregistrement

Cette section affiche:

- **Informations produit** : le produit et la version BitDefender.
- **Informations d'enregistrement** : l'adresse e-mail utilisée pour vous connecter à votre compte BitDefender (si ce dernier est configuré), la clé d'activation actuelle et dans combien de jours la licence arrivera à son terme.

25.1. Enregistrement de BitDefender Antivirus 2010

Cliquez sur **S'enregistrer** pour ouvrir la fenêtre d'enregistrement du produit.


BitDefender Antivirus 2010
Assistant d'enregistrement
Enregistrement de BitDefender
Informations concernant la clé de licence actuelle
Type : VALIDE, VERSION D'ÉVALUATION
Expire dans : 29 jours
Saisir la clé de licence :
Clé de licence :
Saisissez la clé de licence
S'enregistrer
Vous n'avez pas de clé de licence ? Achetez-en une maintenant !
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Suivant

Enregistrement

Vous pouvez visualiser l'état de votre enregistrement BitDefender, votre clé d'activation actuelle ou voir dans combien de jours la licence arrivera à son terme.

Pour enregistrer BitDefender Antivirus 2010 :

1. Entrez la clé d'activation dans le champ de saisie.

   Note
   Vous trouverez votre clé d'activation :
   - sur l'étiquette du CD.
   - sur la carte d'enregistrement du produit.
   - sur l'e-mail d'achat en ligne.

   Si vous n'avez pas de clé d'activation BitDefender, cliquez sur le lien indiqué pour être dirigé vers la boutique en ligne BitDefender et en acheter une.

2. Cliquez sur **S'enregistrer**.
3. Cliquez sur **Terminer**.

25.2. Création d'un compte BitDefender

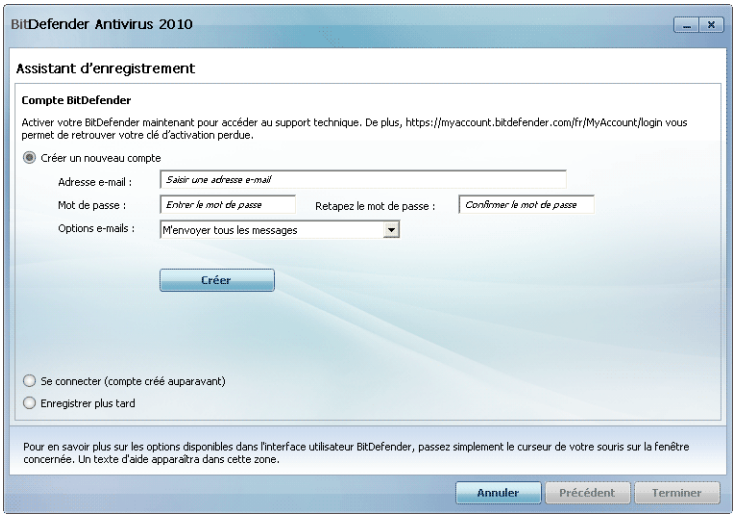
La création d'un compte BitDefender est OBLIGATOIRE pour finaliser l'enregistrement de votre produit BitDefender. Le compte BitDefender vous donne accès au support technique, à des offres spéciales et à des promotions. Si vous perdez votre clé

d'activation BitDefender, vous pouvez la retrouver en vous connectant sur votre compte à l'adresse http://myaccount.bitdefender.com.

Important

Vous devez créer un compte dans les 15 jours après l'installation de BitDefender (si vous l'enregistrez avec une clé de licence, l'expiration est repoussée à 30 jours). Dans le cas contraire, BitDefender ne se mettra plus à jour.

Si vous n'avez pas encore créé de compte BitDefender, cliquez sur **Activer le produit** pour ouvrir la fenêtre d'enregistrement du compte.


BitDefender Antivirus 2010
Assistant d'enregistrement
Compte BitDefender
Activer votre BitDefender maintenant pour accéder au support technique. De plus, https://myaccount.bitdefender.com/fr/MyAccount/login vous permet de retrouver votre clé d'activation perdue.
Créer un nouveau compte
Adresse e-mail :
Saisir une adresse e-mail
Mot de passe :
Entrer le mot de passe
Retapez le mot de passe :
Confirmer le mot de passe
Options e-mails :
M'envoyer tous les messages
Créer
Se connecter (compte créé auparavant)
Enregistrer plus tard
Pour en savoir plus sur les options disponibles dans l'interface utilisateur BitDefender, passez simplement le curseur de votre souris sur la fenêtre concernée. Un texte d'aide apparaîtra dans cette zone.
Annuler
Précédent
Terminer

Création de compte

Si vous ne souhaitez pas créer immédiatement un compte BitDefender, sélectionnez **Enregistrer plus tard** et cliquez sur **Terminer**. Autrement, procédez selon votre situation actuelle :

- « Je n'ai pas de compte BitDefender » (p. 201)
- « J'ai déjà un compte BitDefender » (p. 202)

Je n'ai pas de compte BitDefender

Pour créer un compte BitDefender, suivez ces étapes :

1. Sélectionnez **Créer un nouveau compte**.

2. Tapez les informations requises dans les champs correspondants. Les informations communiquées ici resteront confidentielles.
   - **E-mail** - entrez votre adresse e-mail.
   - **Mot de passe** - entrez un mot de passe pour votre compte BitDefender. Le mot de passe doit contenir entre 6 et 16 caractères.
   - **Retaper le mot de passe** - re-entrez le mot de passe choisi auparavant.

   Note
   Une fois le compte activé, vous pouvez utiliser l'adresse e-mail et le mot de passe indiqués pour vous connecter à votre compte sur http://myaccount.bitdefender.com.

3. Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte. Sélectionnez l'une des options disponibles dans le menu :
   - **M'envoyer tous les messages**
   - **M'envoyer seulement les messages concernant le produit**
   - **Je ne veux recevoir aucun message**
4. Cliquez sur **Créer**.
5. Cliquez sur **Terminer** pour quitter l'assistant.
6. **Activez votre compte.** Vous devez activez votre compte avant de pouvoir l'utiliser. Consultez votre messagerie et suivez les instructions données dans le message que vous a adressé le service d'enregistrement de BitDefender.

J'ai déjà un compte BitDefender

BitDefender détectera automatiquement si vous avez déjà un compte BitDefender actif sur cet ordinateur. Dans ce cas, indiquez le mot de passe de votre compte et cliquez sur **Se connecter**. Cliquez sur **Terminer** pour quitter l'assistant.

Si vous avez déjà un compte actif, mais que BitDefender ne le détecte pas, suivez ces étapes pour enregistrer le produit avec ce compte :

1. Sélectionnez **Se connecter (compte créé auparavant)**.
2. Tapez l'adresse e-mail et le mot de passe de votre compte dans les champs correspondants.

   Note
   Si vous ne souhaitez pas faire de modifications, cliquez sur **Terminer** pour fermer l'assistant.

3. Si vous le souhaitez, BitDefender peut vous tenir informé des offres spéciales et des promotions en utilisant l'adresse email de votre compte. Sélectionnez l'une des options disponibles dans le menu :

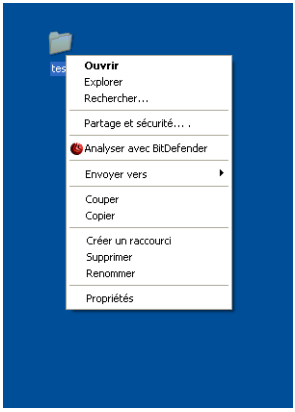
- **M'envoyer tous les messages**
- **M'envoyer seulement les messages concernant le produit**
- **Je ne veux recevoir aucun message**

4. Cliquez sur **Se connecter**.
5. Cliquez sur **Terminer** pour quitter l'assistant.

Intégration dans Windows et dans les logiciels tiers

26. Intégration dans le menu contextuel de Windows

Le menu contextuel de Windows s'affiche si vous faites un clic droit sur un fichier ou un dossier ou sur des objets placés sur votre bureau.



Menu contextuel de Windows

BitDefender s'intègre dans le menu contextuel de Windows pour vous aider à analyser les fichiers et rechercher les virus. Vous pouvez rapidement localiser l'option BitDefender dans le menu contextuel en cherchant l'icône de BitDefender .

26.1. Analyser avec BitDefender

Vous pouvez facilement analyser des fichiers, des dossiers, et même des disques entiers à partir du menu contextuel de Windows. Faites un clic droit sur l'objet que vous souhaitez analyser et sélectionnez **Analyser avec BitDefender** dans le menu. L'Assistant d'analyse antivirus s'affichera et vous guidera pendant le processus d'analyse.

Options d'analyse. Les options d'analyse sont déjà configurées pour que la détection soit la meilleure possible. Si des fichiers infectés sont détectés, BitDefender essaiera de les désinfecter (suppression du code du malware). Si la désinfection échoue, l'assistant d'analyse antivirus vous proposera d'indiquer d'autres moyens d'intervenir sur les fichiers infectés.

Pour modifier les options d'analyse, les étapes sont les suivantes :

1. Ouvrez BitDefender et faites passer l'interface utilisateur en Mode Expert.
2. Cliquez sur **Antivirus** dans le menu de gauche.
3. Cliquez sur l'onglet **Analyse antivirus**.

4. Faites un clic droit sur la tâche **Analyse contextuelle** et sélectionnez **Ouvrir**. Une fenêtre s'affichera.
5. Cliquez sur **Personnaliser** et configurez les options d'analyse suivant vos besoins. Pour savoir ce qu'une option provoque, placez le curseur dessus et lisez la description affichée au bas de la fenêtre.
6. Cliquez **OK** pour sauvegarder les changements.
7. Cliquez sur **OK** pour confirmer et appliquer les nouvelles options d'analyse.

Important
Vous ne devriez pas modifier les options d'analyse de cette méthode à moins d'avoir une très bonne raison de le faire.

27. Intégration dans les navigateurs Internet

BitDefender protège votre ordinateur contre les tentatives de phishing lorsque vous naviguez sur Internet. Il analyse les sites Web auxquels vous accédez et vous prévient en cas de menaces de phishing. Il est possible de configurer une liste blanche de sites Internet qui ne seront pas analysés par BitDefender.

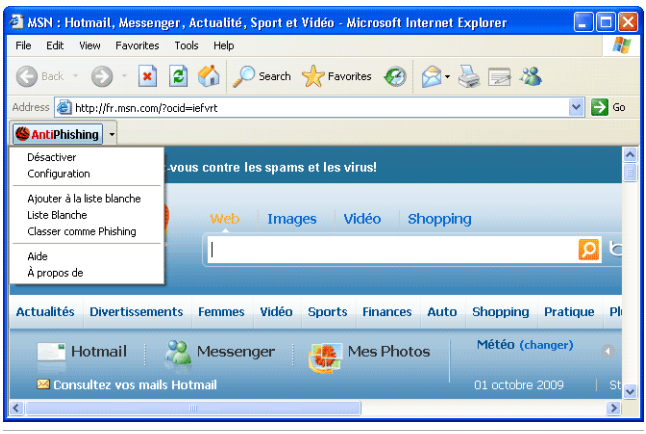
BitDefender s'intègre directement et au moyen d'une barre d'outils intuitive et conviviale aux navigateurs Internet suivants :

- Internet Explorer
- Mozilla Firefox

Vous pouvez gérer facilement et efficacement la protection antiphishing et la liste blanche en utilisant la barre d'outils BitDefender Antiphishing intégrée dans l'un des navigateurs Internet ci-dessus.

La barre d'outils antiphishing, représentée par l'icône BitDefender, est située en haut de la fenêtre du navigateur. Cliquez dessus pour ouvrir le menu de la barre d'outils.

Note
Si vous ne voyez pas la barre d'outils, cliquez sur le menu **Affichage**, sélectionnez **Barres d'outils** et vérifiez **la barre d'outils BitDefender**.



Barre d'outils antiphishing

Les commandes suivantes sont disponibles dans le menu de la barre d'outils :

- **Activer / Désactiver** - active / désactive la protection antiphishing BitDefender dans le navigateur Web actuel.

- **Paramètres** - ouvre une fenêtre où vous pouvez définir les paramètres de la barre d'outils antiphishing. Voici les options proposées :
  - **Protection Web Antipishing en Temps Réel** - détecte et vous prévient en temps réel si un site Web est un site de phishing (conçu pour voler des informations personnelles). Cette option contrôle la protection antiphishing BitDefender uniquement dans le navigateur Web actuel.
  - **Demander avant d'ajouter à une liste blanche** - demande votre autorisation avant d'ajouter un site Web à la liste blanche.
- **Ajouter à la liste blanche** - ajoute le site Web actuel à la liste blanche.

Note
Si vous ajoutez un site Web à la liste blanche, BitDefender n'analysera plus le site pour détecter les tentatives de phishing. Nous vous recommandons d'ajouter uniquement à la liste blanche les sites auxquels vous faites pleinement confiance.

- **Liste Blanche** - ouvre la Liste Blanche.

BitDefender Antivirus 2010
Liste Blanche
Ceci est la liste des URL qui ne seront pas filtrées par les moteurs antiphishing de BitDefender.
Les URL entrées dans la liste blanche ne seront pas analysées par les moteurs antiphishing de BitDefender. Vous ne serez informé(e) d'aucune menace potentielle sur ces pages.
Ajouter URL :
Ajouter
Site Web
fr.msn.com
Supprimer
Vous pouvez définir ici une liste de sites Web (adresses URL) qui ne seront pas analysés par les moteurs antiphishing de BitDefender.
Fermer
Enregistrer

Liste blanche antiphishing

Vous pouvez consulter la liste de tous les sites Web qui ne seront pas analysés par les moteurs BitDefender d'antiphishing. Si vous souhaitez supprimer un site de la liste blanche – pour pouvoir être prévenu de tout risque de phishing sur la page correspondante, cliquez sur le bouton **Supprimer** en regard du nom du site.

Vous pouvez ajouter à la liste blanche les sites auxquels vous faites pleinement confiance, pour qu'ils ne soient plus analysés par les moteurs d'antiphishing. Pour ajouter un site à la liste blanche, entrez son adresse dans le champ correspond et cliquez sur le bouton **Ajouter**.

- **Signaler comme Phishing** - informe les laboratoires BitDefender que vous considérez que le site Web est utilisé pour du phishing. En signalant des sites Web de phishing vous contribuez à protéger d'autres utilisateurs contre le vol d'identité.
- **Aide** - ouvre la documentation électronique.
- **A propos de** - Affichage d'une fenêtre contenant des informations relatives à BitDefender, ainsi que des éléments d'aide si vous rencontrez une situation anormale.

28. Intégration dans les Programmes de Messagerie Instantanée

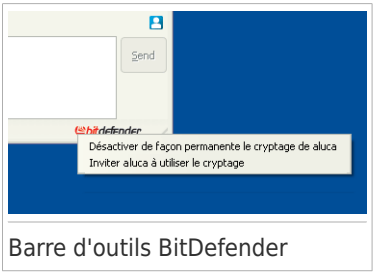
BitDefender dispose d'une fonction de cryptage pour protéger vos documents confidentiels et vos conversations via les messageries instantanées Yahoo Messenger et MSN Messenger.

Par défaut, BitDefender crypte toutes vos sessions de messagerie instantanée, à condition que :

- votre correspondant ait installé sur son ordinateur une version de BitDefender qui prenne en charge le cryptage de messagerie instantanée et que ce dernier soit activé pour l'application de messagerie instantanée utilisée pour converser ;
- vous et votre correspondant utilisiez soit Yahoo Messenger, soit Windows Live (MSN) Messenger.

Important
BitDefender ne cryptera pas la conversation si le correspondant utilise une application à interface Web, telle que Meebo, ou une autre application de chat compatible avec Yahoo Messenger ou MSN.

Vous pouvez aisément configurer le cryptage de messagerie instantanée en utilisant la barre d'outils BitDefender dans la fenêtre de chat. La barre d'outils devrait être située à l'angle inférieur droit de la fenêtre de la conversation. Cherchez le logo BitDefender pour la trouver.



Barre d'outils BitDefender

Note
La barre d'outils indique qu'une conversation est cryptée en affichant une petite clé à côté du logo BitDefender.

En cliquant sur la barre d'outils BitDefender vous obtiendrez les options suivantes :

- **Désactiver en permanence le cryptage pour le contact.**
- **Inviter le contact à utiliser le cryptage.** Pour crypter vos conversations, votre contact doit installer BitDefender et utiliser un programme de Messagerie Instantanée compatible.

Comment faire pour

29. Comment analyser fichiers et dossiers

Avec BitDefender, l'analyse est facile et souple. Il existe 4 façons de paramétrer BitDefender pour qu'il analyse fichiers et dossiers à la recherche de virus et autres malwares :

- Utilisation du menu contextuel de Windows
- Utilisation des tâches d'analyse
- Utilisation de BitDefender Manual Scan
- En utilisant la barre d'activité d'analyse

Quand vous lancez une analyse, l'assistant d'analyse antivirus s'affiche et vous guide pendant tout le processus. Pour plus d'informations sur cet assistant, veuillez consulter « *Assistant d'analyse antivirus* » (p. 55).

29.1. Utilisation du menu contextuel de Windows

C'est le moyen le plus simple conseillé pour analyser un fichier ou un dossier sur votre ordinateur. Faites un clic droit sur l'objet que vous souhaitez analyser et sélectionnez **Analyser avec BitDefender** dans le menu. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse.

Cette méthode d'analyse est à utiliser dans des situations typiques qui englobent les cas suivants :

- Vous soupçonnez un fichier ou un dossier donné d'être infecté.
- Quand vous téléchargez sur Internet des fichiers dont vous pensez qu'ils pourraient être dangereux.
- Analysez un dossier partager sur le réseau avant de copier des fichiers sur votre ordinateur.

29.2. Utilisation des tâches d'analyse

Si vous souhaitez analyser régulièrement votre ordinateur ou des dossiers particuliers, il est préférable d'utiliser les tâches d'analyse. Les tâches d'analyse indique à BitDefender les emplacements à analyser, les options d'analyse à utiliser et les mesures à prendre. En outre, vous pouvez les planifier pour qu'elles s'exécutent à un rythme régulier ou à un moment donné.

Pour analyser votre ordinateur en utilisant les tâches d'analyse, vous devez ouvrir l'interface BitDefender et lancer la tâche d'analyse voulue. En fonction du mode d'affichage de l'interface utilisateur, différentes étapes doivent être suivies pour lancer la tâche d'analyse.

Lancement des tâches d'Analyse en Mode Débutant

En Mode Débutant, vous pouvez seulement lancer une analyse standard de l'ensemble de l'ordinateur en cliquant sur **Analyser**. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse.

Lancement des tâches d'Analyse en Mode Intermédiaire

En Mode Intermédiaire, vous pouvez lancer un certain nombre de tâches d'analyse pré-configurées. Vous pouvez aussi configurer et lancer des tâches d'analyse personnalisées afin d'analyser des emplacements spécifiques de votre ordinateur en utilisant les options d'analyse personnalisées. Pour lancer une tâche d'analyse en Mode Intermédiaire, suivez ces étapes :

1. Cliquez sur l'onglet **Antivirus**.
2. Dans la partie gauche de Tâches Rapides, cliquez sur **Analyse du Système** pour lancer une analyse standard de tout l'ordinateur. Pour lancer une tâche d'analyse différente, cliquez sur la flèche du bouton et sélectionnez la tâche d'analyse souhaitée. Pour configurer et lancer une analyse personnalisée, cliquez sur **Analyse Personnalisée**. Les tâches d'analyse disponibles sont les suivantes :

Tâche d'analyse	Description
Analyse du Système	Analyse l'ensemble du système, mis à part les archives. Dans la configuration par défaut, l'analyse recherche tous les types de malwares à l'exception des rootkits.
Analyse approfondie du système	Analyse l'ensemble du système. La configuration par défaut permet d'analyser tous les types de codes malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse de Mes documents	Utilisez-la pour analyser les dossiers importants de l'utilisateur actuel: `Mes documents`, `Bureau` et `Démarrage`. Cela vous permet d'assurer la sécurité de vos documents, un espace de travail sécurisé et d'exécuter des applications saines au démarrage.
Analyse personnalisée	Cette option vous aide à configurer et à lancer une tâche d'analyse personnalisée en vous permettant de spécifier les éléments à analyser et les options générales d'analyse. Vous pouvez enregistrer des tâches d'analyse personnalisée auxquelles vous pourrez accéder ensuite en Mode Intermédiaire ou en Mode Expert.

3. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse. Si vous avez choisi de lancer une analyse personnalisée, vous devez utiliser l'assistant d'Analyse Personnalisée.

Lancement des tâches d'analyse en Mode Expert

En Mode Expert, vous pouvez lancer toutes les tâches d'analyse pré-configurées et modifier leurs options d'analyse. Vous pouvez également créer des tâches personnalisées si vous souhaitez analyser des emplacements particuliers de votre ordinateur. Pour lancer une tâche d'analyse en Mode Expert, suivez ces étapes :

1. Cliquez sur **Antivirus** dans le menu de gauche.
2. Cliquez sur l'onglet **Analyse antivirus**. Vous pouvez trouver ici les tâches d'analyse par défaut et créer vos propres tâches d'analyse. Les tâches d'analyse par défaut sont les suivantes :

Tâche d'analyse par défaut	Description
Analyse approfondie du système	Analyse l'ensemble du système. La configuration par défaut permet d'analyser tous les types de codes malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse du Système	Analyse l'ensemble du système, mis à part les archives. Dans la configuration par défaut, l'analyse recherche tous les types de malwares à l'exception des rootkits.
Analyse rapide du système	Analyse les dossiers `Windows` et `Program Files` La configuration par défaut permet d'analyser tous les types de codes malveillants, à l'exception des rootkits, mais ne permet pas d'analyser la mémoire, les registres et les cookies.
Mes documents	Utilisez-la pour analyser les dossiers importants de l'utilisateur actuel: `Mes documents`, `Bureau` et `Démarrage`. Cela vous permet d'assurer la sécurité de vos documents, un espace de travail sécurisé et d'exécuter des applications saines au démarrage.

3. Double cliquez sur la tâche d'analyse que vous voulez lancer.
4. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse.

29.3. Utilisation de BitDefender Manual Scan

BitDefender Manual Scan vous permet d'analyser un dossier particulier ou une partition d'un disque dur sans avoir à créer une tâche d'analyse. Cette fonctionnalité est conçue pour être utilisée lorsque Windows a été démarré en Mode sans échec Si votre système est infecté par un virus résistant, vous pouvez essayer de le supprimer en faisant démarrer Windows en Mode sans échec et en faisant analyser chaque partition du disque par BitDefender Manual Scan.

Pour analyser votre ordinateur avec BitDefender Manual Scan, les étapes sont les suivantes :

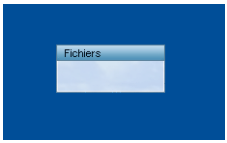
1. Dans le menu Démarrer de Windows, cliquez sur **Démarrer** → **Programmes** → **BitDefender 2010** → **Analyse manuelle BitDefender**. Une nouvelle fenêtre s'affiche.
2. Cliquez sur **Ajouter Dossier** pour sélectionner la cible de l'analyse. Une nouvelle fenêtre s'affiche.
3. Sélectionnez la cible de l'analyse :
   - Pour analyser votre bureau, sélectionnez simplement **Bureau**.
   - Pour analyser un disque dur entier, sélectionnez-le dans Poste de travail.
   - Pour analyser un dossier particulier, recherchez-le et sélectionnez-le.
4. Cliquez sur **OK**.
5. Cliquez sur **Continuer** pour démarrer l'analyse.
6. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse.

Que signifie Mode sans échec ?
Le Mode sans échec est une façon particulière de démarrer Windows, principalement utilisée pour localiser les problèmes affectant le fonctionnement normal de Windows. De tels problèmes peuvent provenir d'un conflit entre pilotes ou de virus empêchant Windows de démarrer normalement. En Mode sans échec, Windows ne charge qu'un minimum de composants du système d'exploitation et les pilotes de base. Il n'existe que quelques applications qui fonctionnent en Mode sans échec. C'est pour cette raison que la plupart des virus sont inactifs et peuvent être facilement supprimés quand Windows est utilisé dans ce mode.
Pour faire démarrer Windows en Mode sans échec, redémarrez votre ordinateur et appuyez sur la touche F8 jusqu'à ce que le menu des fonctions avancées de Windows s'affiche. Vous pouvez choisir entre plusieurs options de démarrage de Windows en Mode sans échec. Vous pourrez sélectionner **Mode sans échec avec réseau** si vous souhaitez pouvoir accéder à Internet.

Note

Pour plus d'informations sur le Mode sans échec, allez dans le centre d'aide et de support de Windows (dans le menu Démarrer, cliquez sur **Aide et support**). Vous pouvez également rechercher des informations sur Internet.

29.4. Utilisation de la barre d'activité d'analyse



Barre de l'activité d'analyse

La **Barre d'analyse d'activité** est une visualisation graphique de l'analyse d'activité de votre système. Cette petite fenêtre est disponible par défaut uniquement dans le Mode Expert.

Vous pouvez utiliser la barre d'activité d'analyse pour analyser rapidement des fichiers et des dossiers. Faites glisser-déposer le fichier ou le dossier que vous souhaitez analyser dans la barre d'activité d'analyse. Suivez les indications de l'assistant de l'analyse antivirus pour effectuer l'analyse.

Note
Pour plus d'informations, reportez-vous à « *Barre de l'activité d'analyse* » (p. 32).

30. Comment planifier l'analyse de l'ordinateur

Analyser régulièrement votre ordinateur est le meilleur moyen de le conserver à l'abri du malware. BitDefender vous permet de planifier des tâches d'analyse qui font que votre ordinateur est analysé automatiquement.

Pour planifier l'analyse de votre ordinateur avec BitDefender, les étapes sont les suivantes :

1. Ouvrez BitDefender et faites passer l'interface utilisateur en Mode Expert.
2. Cliquez sur **Antivirus** dans le menu de gauche.
3. Cliquez sur l'onglet **Analyse antivirus**. Vous pouvez trouver ici les tâches d'analyse par défaut et créer vos propres tâches d'analyse.
   - Des tâches système sont disponibles et peuvent s'exécuter sur n'importe quel compte utilisateur Windows.
   - Seul le créateur des tâches utilisateur peut avoir accès à elles et les lancer.

   Voici les tâches d'analyse par défaut que vous pouvez planifier :

Tâche d'analyse par défaut	Description
Analyse approfondie du système	Analyse l'ensemble du système. La configuration par défaut permet d'analyser tous les types de codes malveillants menaçant la sécurité de votre système, tels que les virus, spywares, adwares, rootkits et autres.
Analyse du Système	Analyse l'ensemble du système, mis à part les archives. Dans la configuration par défaut, l'analyse recherche tous les types de malwares à l'exception des rootkits.
Analyse rapide du système	Analyse les dossiers `Windows` et `Program Files` La configuration par défaut permet d'analyser tous les types de codes malveillants, à l'exception des rootkits, mais ne permet pas d'analyser la mémoire, les registres et les cookies.
Analyse automatique à l'ouverture de session	Analyse les éléments qui sont exécutés quand un utilisateur se connecte à Windows. Pour utiliser cette tâche vous devez la planifier pour qu'elle s'exécute au démarrage du système. Par défaut, l'analyse à l'ouverture de session est désactivée.

Tâche d'analyse par défaut	Description
Mes documents	Utilisez-la pour analyser les dossiers importants de l'utilisateur actuel: `Mes documents`, `Bureau` et `Démarrage`. Cela vous permet d'assurer la sécurité de vos documents, un espace de travail sécurisé et d'exécuter des applications saines au démarrage.

Si aucune de ces tâches d'analyse ne correspond à vos besoins, vous pouvez en créer une nouvelle, que vous pourrez alors programmer pour qu'elle s'exécute selon vos souhaits.

4. Faites un clic droit sur la tâche désirée et sélectionnez **Planifier**. Une nouvelle fenêtre s'affiche.
5. Planifier la tâche pour qu'elle s'exécute comme souhaité :
   - Pour ne lancer la tâche d'analyse qu'une fois, sélectionnez **Une fois** et indiquer la date et l'heure du démarrage.
   - Pour lancer la tâche d'analyse au démarrage du système, sélectionnez **Au démarrage du système**. Spécifiez combien de temps après le démarrage la tâche doit s'exécuter (en minutes).
   - Pour lancer la tâche d'analyse à un rythme régulier, sélectionnez **Périodiquement** et indiquez la fréquence et la date et l'heure du démarrage.

   Note
   Par exemple, pour analyser votre ordinateur tous les samedis à 2 heures du matin, vous devez procéder comme suit :
   a. Sélectionnez **Périodiquement**.
   b. Dans le champ **Tous/Toutes les**, tapez 1, puis sélectionnez **semaines** dans le menu. La tâche s'exécute ainsi une fois par semaine.
   c. Indiquez que la tâche doit débuter samedi prochain.
   d. Indiquez l'heure de début `02.00.00`.
6. Cliquez sur **OK** pour enregistrer la planification. La tâche d'analyse s'exécutera automatiquement au moment que vous aurez planifié. Si l'ordinateur est éteint au moment prévu, la tâche s'exécutera la prochaine fois que vous le rallumerez.

Aide et résolution des problèmes

31. Résolution des problèmes

Ce chapitre présente certains problèmes que vous pouvez rencontrer en utilisant BitDefender et vous fournit des solutions possibles à ces problèmes. La plupart de ces problèmes peuvent être résolus par une configuration appropriée des paramètres du produit.

Si votre problème n'est pas évoqué ici, ou si les solutions proposées ne permettent pas de le régler, vous pouvez contacter le support technique BitDefender comme indiqué dans le chapitre « *Support Technique Editions Profil / BitDefender* » (p. 225).

31.1. Problèmes d'installation

Cet article vous aide à résoudre les problèmes d'installation les plus fréquents avec BitDefender. Ces problèmes peuvent être regroupés dans les catégories suivantes :

- Erreurs de validation de l'installation : l'assistant de configuration ne peut pas être exécuté en raison de conditions spécifiques sur votre système.
- Échec des installations : vous avez lancé une installation à partir de l'assistant de configuration, mais elle n'a pas abouti.

31.1.1. Erreurs de Validation de l'Installation

Lorsque vous lancez l'assistant de configuration, certaines conditions sont vérifiées afin de s'assurer que l'installation peut démarrer. Le tableau suivant présente les erreurs de validation de l'installation les plus fréquentes et les solutions pour les corriger.

Erreur	Description et Solution
Vous n'avez pas suffisamment de privilèges pour installer le programme.	Pour lancer l'assistant de configuration et installer BitDefender, vous avez besoin des privilèges administrateur. Choisissez une des possibilités suivantes : ● Connectez-vous à un compte Windows administrateur et relancez l'assistant de configuration. ● Faites un clic droit sur le fichier d'installation et sélectionnez **Exécuter en tant que**. Tapez le nom d'utilisateur et le mot de passe du compte Windows administrateur de ce système.

Erreur	Description et Solution
Le programme d'installation a détecté une version précédente de BitDefender qui n'a pas été désinstallée correctement.	BitDefender a déjà été installé sur votre système, et n'a pas été complètement désinstallé. Cela empêche une nouvelle installation de BitDefender. Pour corriger cette erreur et installer BitDefender, suivez ces étapes : 1. Sur www.bitdefender.fr/uninstall téléchargez l'outil de désinstallation sur votre ordinateur. 2. Lancez l'outil de désinstallation avec les privilèges administrateur. 3. Redémarrez votre ordinateur. 4. Relancez l'assistant de configuration pour installer BitDefender.
Ce programme BitDefender n'est pas compatible avec votre système d'exploitation.	Vous essayez d'installer BitDefender sur un système d'exploitation non pris en charge. Veuillez consulter « *Configuration requise* » (p. 2) pour savoir sur quels systèmes d'exploitation vous pouvez installer BitDefender. Si votre système d'exploitation est Windows XP avec Service Pack 1 ou sans Service Pack, vous pouvez installer le Service Pack 2 ou supérieur et relancer ensuite l'assistant de configuration.
Le fichier d'installation est conçu pour un autre type de processeur.	Si vous obtenez cette erreur, c'est parce que vous essayez d'exécuter une mauvaise version du fichier d'installation. Il existe deux versions du fichier d'installation BitDefender : l'une pour les processeurs 32 bits et l'autre pour les processeurs 64 bits. Pour être sûr(e) d'avoir la version adaptée à votre système, téléchargez le fichier d'installation directement à partir de www.bitdefender.fr.

31.1.2. L'installation a échoué

Plusieurs raisons peuvent expliquer l'échec de l'installation :

- Pendant l'installation, un écran d'erreur s'affiche. Il se peut qu'on vous demande d'annuler l'installation ou un bouton peut vous proposer un outil de désinstallation pour nettoyer le système.

Note

Juste après avoir lancé l'installation, on peut vous signaler qu'il n'y a pas assez d'espace disque libre pour installer BitDefender. Dans ce cas, libérez l'espace disque demandé sur la partition où vous souhaitez installer BitDefender puis reprenez ou relancez l'installation.

- L'installation s'interrompt et, éventuellement, votre système se bloque. Seul un redémarrage rétablit la réactivité du système.
- L'installation est terminée, mais vous ne pouvez pas utiliser certaines ou toutes les fonctions de BitDefender.

Pour corriger une installation ayant échoué et installer BitDefender, suivez ces étapes :

1. **Nettoyez le système après l'échec de l'installation. .** Si l'installation échoue, certaines clés de registre et fichiers BitDefender peuvent demeurer sur votre système. De tels restes peuvent empêcher une nouvelle installation de BitDefender. Ils peuvent aussi affecter la performance du système et sa stabilité. C'est pourquoi vous devez les supprimer avant d'essayer de réinstaller le programme.

   Si l'écran d'erreur propose un outil de désinstallation, cliquez sur ce bouton pour nettoyer le système. Sinon, procédez comme suit :

   a. Sur www.bitdefender.fr/uninstall téléchargez l'outil de désinstallation sur votre ordinateur.

   b. Lancez l'outil de désinstallation avec les privilèges administrateur.

   c. Redémarrez votre ordinateur.

2. **Vérifiez les causes pouvant expliquer l'échec de l'installation. .** Avant de réinstaller le programme, vérifiez que l'échec de l'installation n'est pas dû aux conditions suivantes :

   a. Vérifiez que vous n'avez pas d'autre solution de sécurité installée car cela pourrait affecter le fonctionnement normal de BitDefender. Si c'est le cas, nous vous recommandons de supprimer toutes les autres solutions de sécurité et de réinstaller ensuite BitDefender.

   b. Vous devriez également vérifier que votre système n'est pas infecté. Choisissez une des possibilités suivantes :

      - Utilisez le CD de Secours BitDefender pour analyser votre ordinateur et supprimer toutes les menaces présentes. Pour plus d'informations, reportez-vous à « BitDefender Rescue CD » (p. 228).
      - Ouvrez une fenêtre Internet Explorer, allez sur www.bitdefender.fr et lancez une analyse en ligne (cliquez sur **Analyse en ligne**).

3. Réessayez d'installer BitDefender. Nous vous recommandons de télécharger et d'exécuter la dernière version du fichier d'installation à partir de www.bitdefender.fr.
4. Si l'installation échoue de nouveau, contactez le support BitDefender comme indiqué dans « *Support Technique Editions Profil / BitDefender* » (p. 225).

31.2. Le Services BitDefender ne répondent pas

Cet article vous aide à régler l'erreur *Les Services BitDefender ne répondent pas*. Vous pouvez rencontrer cette erreur de la façon suivante :

- L'icône BitDefender de la zone de notification est grisée et une fenêtre pop-up vous informe que les services BitDefender ne répondent pas.
- La fenêtre BitDefender indique que les services BitDefender ne répondent pas.

L'erreur peut être causée par :

- une mise à jour importante est en cours d'installation.
- erreurs de communication temporaires entre les services BitDefender.
- certains services BitDefender sont interrompus.
- d'autres solutions de sécurité sont en cours d'exécution sur votre ordinateur en même temps que BitDefender.
- des virus sur votre système affectent le fonctionnement de BitDefender.

Pour régler cette erreur, essayez ces solutions :

1. Attendez quelques instants et voyez si quelque chose change. L'erreur peut être temporaire.
2. Redémarrez l'ordinateur et attendez quelques instants jusqu'à ce que BitDefender soit chargé. Ouvrez BitDefender pour voir si l'erreur persiste. Redémarrer l'ordinateur règle habituellement le problème.
3. Vérifiez que vous n'avez pas d'autre solution de sécurité installée car cela pourrait affecter le fonctionnement normal de BitDefender. Si c'est le cas, nous vous recommandons de supprimer toutes les autres solutions de sécurité et de réinstaller ensuite BitDefender.
4. Si l'erreur persiste, il se peut qu'il y ait un problème plus sérieux (il se peut par exemple que vous soyez infecté par un virus qui interfère avec BitDefender). Veuillez contacter le support BitDefender comme indiqué dans la section « *Support Technique Editions Profil / BitDefender* » (p. 225).

31.3. La désinstallation de BitDefender a échoué

Cet article vous aide à régler les erreurs pouvant se produire lors de la désinstallation de BitDefender. Deux situations sont possibles :

- Pendant la désinstallation, un écran d'erreur s'affiche. L'écran comporte un bouton permettant de lancer un outil de désinstallation pour nettoyer le système.
- La désinstallation s'interrompt et, éventuellement, votre système se bloque. Cliquez sur **Annuler** pour abandonner la désinstallation. Si cela ne fonctionne pas, redémarrez le système.

Si la désinstallation échoue, certaines clés de registre et fichiers BitDefender peuvent demeurer sur votre système. De tels restes peuvent empêcher une nouvelle installation de BitDefender. Ils peuvent aussi affecter la performance du système et sa stabilité. Pour désinstaller complètement BitDefender de votre système, vous devez lancer l'outil de désinstallation.

Si la désinstallation échoue et qu'un écran d'erreur s'affiche, cliquez sur le bouton permettant de lancer l'outil de désinstallation pour nettoyer le système. Sinon, procédez comme suit :

1. Sur www.bitdefender.fr/uninstall téléchargez l'outil de désinstallation sur votre ordinateur.
2. Lancez l'outil de désinstallation avec les privilèges administrateur. L'outil de désinstallation efface tous les fichiers ainsi que les clés d'enregistrement qui n'ont pas été supprimés lors de la désinstallation automatique.
3. Redémarrez votre ordinateur.

Si ces informations ne vous ont pas aidé(e), vous pouvez contacter le support BitDefender comme indiqué dans la section « *Support Technique Editions Profil / BitDefender* » (p. 225).

32. Support Technique Editions Profil / BitDefender

Centre d'Assistance des Laboratoires Technologiques et Scientifiques

Les Laboratoires d'Editions Profil et de BitDefender assurent un niveau d'assistance sur tous les produits maintenus par l'équipe de développement. La résolution d'un problème peut nous amener à vous proposer de mettre gratuitement à niveau la version de votre produit.

Ce service offre une assistance pour les questions ou problèmes liés à des applications courantes pour l'utilisateur final ou les entreprises, telles que :

- Des configurations personnalisées des produits BitDefender.
- Des conseils de prise en main en monoposte ou en relation avec des réseaux simples.
- Des problèmes techniques après l'installation des produits BitDefender.
- Des aides afin de contrer les activités de codes malicieux présents sur un système.
- L'accès à notre site internet de maintenance personnalisée et de FAQ en ligne 24h/24 et 7j/7 : http://supportbd.fr
- L'accès aux informations des centres de support internationaux, qui permettent de gérer les situations par chat online – Accessible 7j/7 – 365j/an. Pour y accéder, veuillez saisir l'adresse ci-dessous dans votre navigateur : http://www.bitdefender.fr/site/KnowledgeBase/liveAssistance. Attention : ce module est un service international, assuré majoritairement en Anglais.

Assistance téléphonique :

Les Laboratoires Editions Profil et BitDefender mettent en oeuvre tous les efforts commercialement envisageables pour maintenir l'accès à l'assistance téléphonique de ce service, pendant les heures ouvrées locales du lundi au vendredi, sauf pendant les jours fériés.

Accès téléphoniques aux Laboratoires Editions Profil et BitDefender :

- **Pour la France et les DOM-TOM** : 0892 561 161 (0.34 euros / minute)
- **Pour la Belgique** : 070 35 83 04
- **Pour la Suisse** : 0900 000 118 (0,60 FS / minute)

Avant de nous appeler, munissez-vous :

- du numéro de licence du produit BitDefender. Communiquez le à un de nos analystes afin qu'il vérifie votre niveau d'assistance.
- de la version actuelle du système d'exploitation.
- des informations sur les marques et modèles de tous les périphériques et des logiciels chargés en mémoire ou utilisés.

En cas d'infection, l'analyste pourra demander une liste d'informations techniques à fournir ainsi que certains fichiers, qui pourront être nécessaires à son diagnostic.

Lorsqu'un analyste vous le demande, précisez les messages d'erreurs reçus et le moment où ils apparaissent, les activités qui ont précédées le message d'erreur et les démarches déjà entreprises pour résoudre le problème.

L'analyste suivra une procédure de dépannage stricte afin de tenter de diagnostiquer le problème.

Le Service n'inclut pas les éléments suivants :

- Ce service d'assistance ne comprend pas les applications, les installations, la désinstallation, le transfert, la maintenance préventive, la formation, l'administration à distance ou configurations logicielles autres que celles spécifiquement notifiées par l'analyste des Laboratoires Editions Profil et BitDefender lors de l'intervention.
- L'installation, le paramétrage, l'optimisation et la configuration en réseau ou à distance d'applications n'entrant pas dans le cadre de l'assistance actuelle.
- Sauvegarde des logiciels/données. Il incombe au Client d'effectuer une sauvegarde de toutes les données, des logiciels et des programmes existants sur les systèmes d'information pris en charge avant toute prestation de service par Editions Profil et de BitDefender.

Edtions Profil ou BitDefender NE PEUVENT ÊTRE TENUS RESPONSABLE DE LA PERTE OU DE LA RÉCUPÉRATION DE DONNÉES, DE PROGRAMMES, OU DE LA PRIVATION DE JOUISSANCE DES SYSTÈME(S) OU DU RÉSEAU.

Les conseils sont strictement limités aux questions demandées et basées sur les informations fournies par le client. Les problèmes et les solutions peuvent dépendre de la nature de l'environnement du système et d'une variété d'autres paramètres qui sont inconnus à Editions Profil ou BitDefender. Par conséquent, Editions Profil ou BitDefender ne peuvent en aucun cas être tenus responsable de dommages résultant de l'utilisation de ces informations.

Il est possible que l'état du système sur lequel les produits BitDefender doivent être installés soit instable (infection préalable, installation d'antivirus ou solutions de sécurité multiples, etc.). Dans ces cas précis, il est possible que l'analyste vous propose une prestation de maintenance auprès de votre revendeur avant de pouvoir régler votre problème.

Les informations techniques peuvent changer lorsque des nouvelles données deviennent disponibles, par conséquent, Editions Profil et BitDefender recommandent que vous consultiez régulièrement notre site "Produits" à l'adresse suivante : http://www.bitdefender.fr pour des mises à jour, ou notre site internet de FAQ à l'adresse http://supportbd.fr.

Tout dommage direct, indirect, spécial, accidentel ou conséquent en relation avec l'usage des informations fournies ne peuvent pas être imputés à Editions Profil et BitDefender.

Si une intervention sur site est nécessaire, l'analyste vous donnera de plus amples instructions concernant votre revendeur le plus proche.

BitDefender Rescue CD

33. Présentation

BitDefender Antivirus 2010 est fourni avec un CD bootable (CD de secours BitDefender), capable d'analyser et désinfecter tous les disques durs existants avant que votre système d'exploitation ne démarre.

Il est recommandé d'utiliser le CD de secours BitDefender à chaque fois que votre système d'exploitation ne fonctionne pas correctement à cause d'une infection virale. Ceci se produit généralement quand vous n'utilisez pas un produit antivirus.

La mise à jour de la base de signatures de virus se fait automatiquement, sans intervention de l'utilisateur, à chaque fois que vous lancez le CD de secours BitDefender.

Le CD de secours BitDefender est une distribution Knoppix remasterisée de BitDefender qui intègre les dernières solutions de sécurité BitDefender pour Linux dans le Live CD de GNU/Linux Knoppix, offrant un antivirus pour poste de travail capable d'analyser et de désinfecter les disques durs (y compris les partitions Windows NTFS). Le CD de secours BitDefender peut aussi être utilisée pour restaurer toutes vos données importantes lorsque Windows ne démarre pas.

Note

Le CD de secours BitDefender peut être téléchargé à partir de cette adresse: http://download.bitdefender.com/rescue_cd/

33.1. Configuration requise

Avant de booter sur le CD de secours BitDefender, vous devez d'abord vérifier que votre système remplit les conditions suivantes :

Type de processeur

x86 compatible, minimum 166 MHz pour des performances minimales, un processur de la génération i686 à 800MHz au moins sera un meilleur choix.

Mémoire

Mémoire minimum: 512Mo de RAM (1 Go recommandés)

CD-ROM

Le CD de secours BitDefender démarre à partir d'un CD-ROM, vous devez donc en posséder un et avoir un BIOS capable de booter depuis ce CD.

Connexion directe à Internet

Bien que le CD de secours BitDefender puisse être exécuté sans connexion Internet, le processus de mise à jour nécéssite un lien HTTP actif pour se télécharger et assurer la meilleure protection possible, même à travers un serveur proxy. La connexion Internet est donc indispensable.

Résolution graphique

Carte graphique standard compatible SVGA.

33.2. Logiciels inclus

Le CD de secours BitDefender inclut le package de logiciels suivant:

Xedit
Il s'agit d'un éditeur de fichier texte.

Vim
C'est un éditeur puissant comportant la mise en évidence de la syntaxe, une IUG et plus encore. Pour plus d'informations, veuillez consulter la page d'accueil de Vim.

Xcalc
Il s'agit d'un calculateur.

RoxFiler
RoxFiler est un gestionnaire de fichiers graphiques rapide et puissant.

Pour plus d'informations, veuillez consulter la page d'accueil de RoxFiler.

MidnightCommander
GNU Midnight Commander (mc) est un gestionnaire de fichiers en mode texte.

Pour plus d'informations, veuillez consulter la page d'accueil de MC.

Pstree
Pstree affiche les processus en cours d'exécution.

Top
Top affiche les tâches Linux.

Xkill
Xkill supprime un client par ses ressources X.

Partition Image
Partition Image vous aide à sauvegarder les partitions aux formats de système de fichiers EXT2, Reiserfs, NTFS, HPFS, FAT16 et FAT32 dans un fichier image. Ce programme peut être utilisé à des fins de sauvegarde.

Pour plus d'informations, veuillez consulter la page d'accueil de Partimage.

GtkRecover
GtkRecover est une version GTK du programme recover. Il permet de restaurer des fichiers.

Pour plus d'informations, veuillez consulter la page d'accueil de GtkRecover.

ChkRootKit
ChkRootKit est un outil qui permet de rechercher les rootkits de votre ordinateur.

Pour plus d'informations, veuillez consulter la page d'accueil de ChkRootKit.

Nessus Network Scanner
Nessus est un moteur d'analyse de sécurité à distance pour Linux, Solaris, FreeBSD et Mac OS X.

Pour plus d'informations, veuillez consulter la page d'accueil de Nessus.

Iptraf
Iptraf est un logiciel de contrôle des réseaux IP.

Pour plus d'informations, veuillez consulter la page d'accueil d'Iptraf.

Iftop
Iftop affiche la bande passante sur une interface.

Pour plus d'informations, veuillez consulter la page d'accueil d'Iftop.

MTR
MTR est un outil de diagnostic réseau.

Pour plus d'informations, veuillez consulter la page d'accueil de MTR.

PPPStatus
PPPStatus affiche des statistiques sur le trafic TCP/IP entrant et sortant.

Pour plus d'informations, veuillez consulter la page d'accueil de PPPStatus.

Wavemon
Wavemon est une application de contrôle des périphériques réseau sans fil.

Pour plus d'informations, veuillez consulter la page d'accueil de Wavemon.

USBView
USBView affiche des informations sur les appareils connectés au bus USB.

Pour plus d'informations, veuillez consulter la page d'accueil USBView.

Pppconfig
Pppconfig permet de configurer automatiquement une connexion ppp commutée.

DSL/PPPoe
DSL/PPPoe configure une connexion PPPoE (ADSL).

I810rotate
I810rotate active et désactive la sortie vidéo du matériel i810 à l'aide de l'outil i810switch(1).

Pour plus d'informations, veuillez consulter la page d'accueil de I810rotate.

Mutt
Mutt est un client de messagerie texte MIME puissant.

Pour plus d'informations, veuillez consulter la page d'accueil de Mutt.

Mozilla Firefox
Mozilla Firefox est un navigateur Web bien connu.

Pour plus d'informations, veuillez consulter la page d'accueil de Mozilla Firefox.

Elinks

Elinks est un navigateur Web en mode texte.

Pour plus d'informations, veuillez consulter la page d'accueil d'Elinks.

34. Comment utiliser le CD de secours BitDefender

Ce chapitre vous explique comment démarrer et arrêter le CD de secours BitDefender, analyser votre ordinateur contre les codes malveillants et enregistrer les données de votre PC sur un support amovible si cela s'avère nécessaire. Les applications logicielles qui accompagnent le CD vous offriront la possibilité d'effectuer de nombreuses tâches, mais leur description dépasse toutefois largement le cadre de ce guide d'utilisation.

34.1. Démarrer le CD de secours BitDefender

Pour lancer le CD, configurez les options de votre BIOS pour autoriser le boot sur le CD au démarrage de l'ordinateur, mettez le CD dans le lecteur et redémarrez. Vérifiez bien que votre ordinateur puisse booter sur un CD.

Patientez jusqu'à l'apparition du prochain message et suivez les instructions pour démarrer le CD de secours BitDefender.

Page d'accueil au démarrage

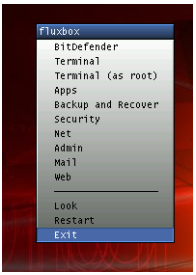
Au démarrage, la mise à jour des signatures de virus est effectuée automatiquement. Cela peut prendre un certain temps.

Quand le processus de démarrage sera terminé, vous pourrez utiliser l'interface du CD de secours BitDefender.

L'interface

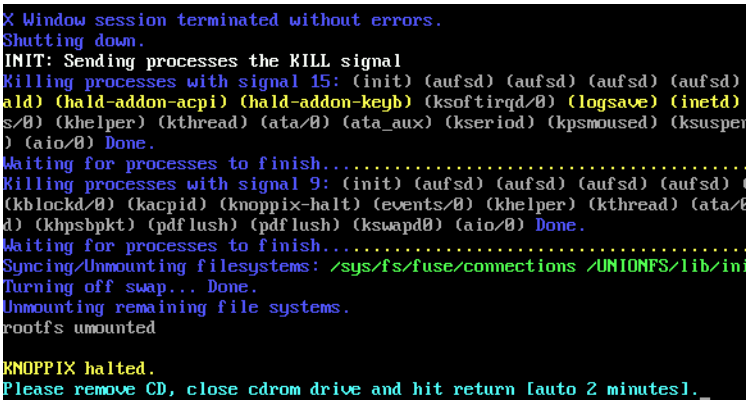
34.2. Arrêter le CD de secours BitDefender

Vous pouvez éteindre votre ordinateur en toute sécurité en sélectionnant **Quitter** dans le menu contextuel du CD de secours BitDefender (double-cliquez pour l'ouvrir) ou en lançant la commande **Arrêt** depuis un terminal.



Choisissez "Sortir"

Lorsque le CD de secours BitDefender a terminé de fermer tous les programmes, il affiche un écran similaire à l'illustration suivante. Vous pourrez retirer le CD pour démarrer depuis votre disque dur. Vous pouvez maintenant éteindre votre ordinateur ou le redémarrer.


X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspe
) (aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/
d) (khpsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs umounted
KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].

Patientez jusqu'à l'apparition de ce message quand vous fermez le programme.

34.3. Comment lancer une analyse antivirus ?

Un assistant apparaitra lorsque le processu sde démarrage sera terminé et vous permettra de lancer une analyse complète de votre ordinateur. Tout ce que vous avez à faire est de cliquer sur le bouton **Start**.

Note
Si la résolution de votre écran n'est pas suffisante, il vous sera demander de commencer l'analyse en mode texte.

Suivez cette procédure en trois étapes pour effectuer le processus d'analyse:

1. Le statut et les statistiques de l'analyse s'affichent (vitesse d'analyse, temps écoulé, nombre d'objets analysés / infectés / suspects / cachés, etc.).

   Note
   L'analyse peut durer un certain temps, suivant sa complexité.

2. Le nombre de problèmes de sécurité affectant votre système est indiqué.

   Les problèmes de sécurité sont affichés en groupes. Cliquez sur "+" pour ouvrir un groupe ou sur "-" pour fermer un groupe.

   Vous pouvez sélectionner une action globale à mener pour chaque groupe de problèmes de sécurité ou sélectionner des actions spécifiques pour chaque problème.
3. Le récapitulatif des résultats s'affiche.

Si vous souhaitez analyser seulement un répertoire spécifique, vous pouvez utiliser l'une des méthodes suivantes :

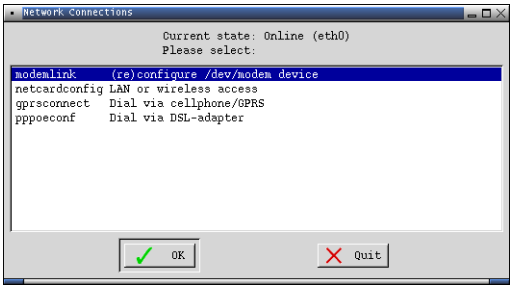
- Utilisez **BitDefender Scanner for Unices**.
  1. Faites un double-clic sur l'icône LANCER SCANNER du Bureau. Cela lancera **BitDefender Scanner for Unices**.
  2. Cliquez sur **Scanner**, une nouvelle fenêtre apparaîtra.
  3. Sélectionez le répertoire que vous souhaitez analyser et cliquez sur **Ouvrir** pour commencer l'analyse en utilisant l'assistant qui est apparu lorsque vous avez démarré l'ordinateur la première fois.
- Utilisez le menu contextuel - parcourez vos dossiers, faites un clic droit sur un fichier ou un répertoire et sélectionnez **Envoyer à**. Puis, choisissez **BitDefender Scanner**.
- Vous pouvez également lancer les commandes suivantes depuis un terminal. Le moteur d'analyse **BitDefender Antivirus Scanner** considérera le fichier ou dossier sélectionné comme étant l'endroit à analyser par défaut.

```
# bdscan /path/to/scan/
```

34.4. Comment configurer la connexion Internet?

Si vous utilisez un réseau DHCP et une carte réseau ethernet, la connexion Internet devrait déjà être reconnue et configurée. Pour la configurer manuellement, suivez les étapes indiquées :

1. Double-cliquez sur le raccourci de connexions Réseau, disponible sur le bureau Windows, la fenêtre suivante apparaîtra.



Connexions réseau

2. Choisissez le type de connexion que vous utilisez et cliquez sur OK.

Connexion	Description
modemlink	Choisissez le type de connexion lorsque vous utilisez un modem et une ligne téléphonique pour accéder à Internet.
netcardconfig	Choisissez ce type de connexion lorsque vous utilisez un Réseau local (LAN) pour accéder à Internet. Ceci s'applique également dans le cas d'une connexion Wi-Fi.
gprsconnect	Choisissez ce type de connexion quand vous accédez à Internet via un réseau de téléphonie mobile en utilisant le protocole GPRS (General Packet Radio Service). Ceci s'applique aussi à l'utilisation de modem GPRS.
pppoeconf	Choisissez ce type de connexion quand vous utilisez un Modem xDSL (Digital Subscriber Line) pour accéder à Internet.

3. Suivez les instructions à l'écran. En cas de doute sur vos réponses, contacter votre administrateur réseau pour plus d'informations.

Important
Merci de noter que les options ci-dessus ne permettent d'activer que le Modem. Pour configurer la connexion Réseau suivez les étapes indiquées.

1. Faîtes un clic-droit sur le bureau. Le menu contextuel du CD de Secours BitDefender apparaîtra.
2. Sélectionnez **Terminal (as root)**.
3. Saisissez les lignes de commande suivantes :

```
# pppconfig
```

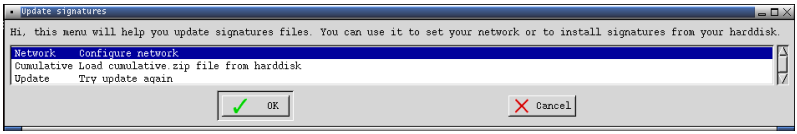
4. Suivez les instructions à l'écran. En cas de doute sur vos réponses, contacter votre administrateur réseau pour plus d'informations.

34.5. Comment actualiser BitDefender?

Lors du démarrage, la mise à jour des signatures de virus est automatique. Cependant, si vous avez sauté cette étape ou souhaitez simplement mettre à jour BitDefender après le démarrage, voici deux façons de procéder.

- Utilisez **BitDefender Scanner for Unices**.
  1. Faites un double-clic sur l'icône LANCER SCANNER du bureau. Cela lancera **BitDefender Scanner for Unices**.
  2. Cliquez sur **Mise à jour**.
- Utilisez le raccourci **Mettre à jour les Signatures** sur le Bureau.

1. Double-cliquez sur le raccourci Mise à jour de Signatures. La fenêtre suivante apparaîtra:


Update signatures
Hi, this menu will help you update signatures files. You can use it to set your network or to install signatures from your harddisk.
Network Configure network
Cumulative Load cumulative zip file from harddisk
Update Try update again
OK
Cancel

Mettre à jour les Signatures

2. Choisissez une des possibilités suivantes :
   - Choisissez **Cumulative** pour parcourir votre disque dur et installer les signatures déjà sauvegardées sur votre disque dur en chargeant le fichier`cumulative.zip`.
   - Choisissez **Mettre à Jour** pour vous connecter immédiatement à Internet et téléchargez la dernière base de signatures.
3. Cliquez sur **OK**.

34.5.1. Comment actualiser BitDefender via un proxy ?

S'il y a un serveur proxy entre votre ordinateur et Internet, certaines configurations doivent être faites pour mettre à jour les signatures de virus.

Pour mettre à jour BitDefender avec un proxy, utilisez l'une des options suivantes :

- Utilisez **BitDefender Scanner for Unices**.
  1. Faites un double-clic sur l'icône LANCER SCANNER du Bureau. Cela lancera **BitDefender Scanner for Unices**.
  2. Cliquez sur **Paramètres**, une nouvelle fenêtre s'affichera.
  3. Sous **Paramètres de Mise à jour**, cochez la case **Activer le Proxy HTTP** Indiquez l'hôte Proxy (à spécifier comme suit : `hôte[:port]`), l'utilisateur Proxy (à spécifier comme suit : `[domaine\]nom d'utilisateur`)et le mot de passe. Cochez la case **Contourner le serveur proxy lorsqu'il n'est pas disponible** pour utiliser une connexion directe lorsque le serveur proxy n'est pas disponible.
  4. Cliquez sur **Enregistrer**
  5. Cliquez sur **Mise à jour**
- Utiliser le Terminal (comme root).
  1. Faîtes un clic-droit sur le bureau. Le menu contextuel du CD de Secours BitDefender apparaîtra.
  2. Sélectionnez **Terminal (as root)**.
  3. Tapez la commande : **cd /ramdisk/BitDefender-scanner/etc**.
  4. Tapez la commande : **mcedit bdscan.conf** pour éditer ce fichier en utilisant GNU Midnight Commander (mc).

5. Pour la ligne suivante : `#HttpProxy =` (just delete the # sign) spécifiez le domaine, le nom d'utilisateur, le mot de passe et le port du serveur proxy. Par exemple, la ligne en question doit ressembler à cela :

   ```
   HttpProxy = myuser:mypassword@proxy.company.com:8080
   ```
6. Tapez sur **F2** pour enregistrer le fichier en cours, confirmer la sauvegarde, et tapez sur **F10** pour le fermer.
7. Tapez la commande : **bdscan update**.

34.6. Comment enregistrer mes données ?

Imaginons que vous ne puissiez pas démarrer votre session Windows en raison d'un problème inexpliqué et que vous deviez à tout prix accéder à des données importantes se trouvant dans votre ordinateur. c'est ici que le CD de secours BitDefender vous sera utile.

Pour enregistrer vos données sur un support amovible, comme une carte mémoire flash USB, procédez comme suit:

1. Insérez le CD de secours BitDefender dans le lecteur CD, la carte mémoire flash dans le lecteur USB, puis redémarrez l'ordinateur.

   Note

   Si vous branchez une clé USB à un autre moment, il vous faudra monter le disque amovible en suivant ces étapes :

   a. Double-cliquez sur le raccourci Terminal Emulator sur le bureau Windows.

   b. Saisissez la commande suivante :

   ```
   # mount  /media/sdb1
   ```

   Merci de noter que selon la configuration de votre ordinateur cela peut être `sda1` au lieu de `sdb1`.

2. Patientez jusqu'à ce que le CD de secours BitDefender finisse de démarrer. La fenêtre suivante apparaît:

Écran du bureau

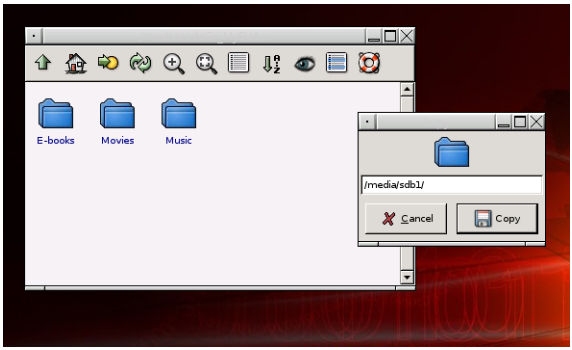
3. Double-cliquez sur la partition où se trouvent les données que vous souhaitez enregistrer (par ex., `[sda3]`).

   Note
   En utilisant le CD de secours BitDefender, vous rencontrerez des noms de partition de type Linux. Ainsi, `[sda1]` correspondra probablement à la partition `(C:)` de type Windows, `[sda3]` à `(F:)` et `[sdb1]` à la carte mémoire flash.

   Important
   Si l'ordinateur n' a pas été éteint correctement il est possible que certaines partitions n'aient pas été montées automatiquement. Pour monter une partition, suivez ces étapes :
   a. Double-cliquez sur le raccourci Terminal Emulator sur le bureau Windows.
   b. Saisissez la commande suivante :

   ```
   # mount  /media/partition_name
   ```

4. Parcourez vos dossiers et ouvrez le répertoire souhaité. Par exemple, `MesDonnées`, qui contient les sous répertoires `Vidéos`, `Musique` et `Livres électroniques`.
5. Faites un clic droit sur le répertoire souhaité, puis sélectionnez **Copier**. La fenêtre suivante apparaît:



Enregistrement des données

6. Saisissez `/media/sdb1/` dans la zone texte correspondante, puis cliquez sur **Copier**.

   Merci de noter que selon la configuration de votre ordinateur cela peut être `sda1` au lieu de `sdb1`.

34.7. Comment utiliser le mode console ?

Si la résolution de votre écran n'est pas suffisante pour l'interface graphique utilisateur, vous pouvez exécuter le CD de secours BitDefender en mode console. Le mode texte simple vous permet de réaliser une analyse complète de votre ordinateur.

Pour lancer le CD en mode console, configurez le BIOS de votre ordinateur pour qu'il démarre à partir du CD, placez le CD dans le lecteur et redémarrez l'ordinateur. Attendez que la page d'accueil apparaisse et sélectionnez **Lancer knoppix en mode console**.

Après le démarrage, suivez les instructions à l'écran pour réaliser une analyse complète de votre ordinateur.

BitDefender détecte les partitions de votre disque dur et met à jour automatiquement la base de données des signatures de malwares avant que l'analyse ne démarre. Si des fichiers infectés sont trouvés, BitDefender les désinfecte. Une fois le processus d'analyse terminé, le journal s'affiche.

Note
L'analyse peut durer un certain temps, suivant sa complexité.

Glossaire

ActiveX

ActiveX est un modèle pour écrire des programmes tels que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour faire des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent demander ou répondre à des questions, utiliser des boutons et interagir d'autres façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic.

Active X est connu pour son manque total de commandes de sécurité ; les experts en sécurité informatique déconseillent son utilisation sur Internet.

Adware

Les adwares sont souvent associés à des applications gratuites ce qui implique leur acceptation par l'utilisateur. Ces adwares étant généralement installés après que l'utilisateur en a accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux.

Cependant les « pop up » publicitaires peuvent devenir contrariant et dans certains cas dégrader les performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui ne s'étaient pas complètement rendu compte des termes de l'accord de licence.

Archive

Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés.

Un fichier qui contient un ou plusieurs fichiers dans un format compressé.

Backdoor

Il s'agit d'une faille dans la sécurité d'un système délibérément laissé en place par des développeurs ou mainteneurs. La motivation n'est pas toujours négative ; quelques logiciels permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.

Secteur de boot

Un secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge la plate-forme.

Virus de boot

Un virus qui infecte le secteur de boot d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus de boot rendra le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.

Navigateur

Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les deux navigateurs les plus populaires sont Netscape Navigator et Microsoft Internet Explorer. Les deux sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plugins) pour certains formats.

Ligne de commande

Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.

Cookies

Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une épée à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent (vous voyez seulement des annonces vous intéressant) mais d'autre part, cela implique en réalité "le pistage" et "le suivi" d'où vous allez et de ce sur quoi vous cliquez sur Internet. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent ainsi considérés comme un simple " numéro SKU " (vous savez, le code barres à l'arrière des produits). Bien que ce point de vue puisse paraître extrême, dans certains cas cette perception est justifiée.

Disk drive

C'est une appareil qui lit et écrit des données sur un disque.

Une unité de disque dur lit et écrit sur un disque dur.

Un lecteur de disquette accède à des disquettes.

Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).

Télécharger

Copier des données (généralement un fichier entier) d'une source principale à un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.

Messagerie électronique

Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.

Événements

Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme l'analyse de la mémoire.

Fausse alerte

Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.

Extension de fichier

La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier.

De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS Dos. Elles comportent communément une à trois lettres (certains vieux OS ne supportent pas plus de trois). Exemples : "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.

Heuristique

Méthode permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique est de pouvoir détecter des variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.

IP

Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP chargé de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.

Applette Java

Il s'agit d'un programme Java conçu pour s'exécuter seulement dans une page Web. Pour utiliser un applet dans une page Web, vous devez spécifier le nom de l'applet et la taille (la longueur et la largeur - en pixels) qu'il peut utiliser. Lors d'un accès à la page Web, le navigateur télécharge l'applet depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les applets diffèrent des applications par le fait qu'ils sont régis par un protocole de sécurité strict.

Par exemple, bien que les applets s'exécutent sur le client, ils ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les applets sont également limités pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.

Virus Macro

Un type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent des langages macro.

Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.

Client de messagerie
Un client de messagerie est un logiciel qui vous permet d'envoyer et recevoir des messages (e-mails).

Mémoire
Zone de stockage interne dans votre ordinateur. Le terme mémoire regarde le stockage des données dans les "chips" (composants), et le terme stockage regarde les disques. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.

Non-heuristique
Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut paraître un virus et ne génère donc pas de fausses alertes.

Programmes empaquetés
Un fichier comprimé. Beaucoup de plates-formes et applications contiennent des commandes vous permettant de comprimer un fichier pour qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide". Normalement, cela nécessite 10 octets.

Pourtant, un logiciel qui comprime les fichiers remplace la série d'espaces par un caractère spécial série d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. C'est juste une technique de compression, il y en a une multitude.

Chemin
Les directions exactes vers un fichier. Ces directions sont décrites d'habitude par arborescence, de haut en bas.

La connexion entre deux points, telle le canal de communication entre deux ordinateurs.

Phishing
Action d'envoyer un e-mail à un utilisateur en prétendant être une entreprise connue dans le but d'obtenir frauduleusement des informations privées qui permettront d'utiliser l'identité du destinataire du mail. Cet e-mail dirige l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.

Virus polymorphique
Un virus qui change de forme avec chaque fichier qu'il infecte. Comme ils n'ont pas une forme unique bien définie, ces virus sont plus difficiles à identifier.

Port

Une interface de l'ordinateur à laquelle vous pouvez connecter un périphérique. Les PCs comportent plusieurs sortes de ports. A l'intérieur, il y a quelques ports pour la connexion des disques, cartes vidéo. A l'extérieur, les PCs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques.

Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.

Fichier journal (Log)

Un fichier qui enregistre les actions qui surviennent. BitDefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.

Rootkit

Un rootkit est un ensemble d'outils logiciels permettant aux administrateurs d'accéder à un système. Le terme a été utilisé initialement pour les systèmes d'exploitation UNIX se réfère à des outils recompilés fournissant des droits administrateurs "intrusifs", permettant de cacher leur présence aux administrateurs systèmes.

Le principale rôle des rootkits est de cacher des processus, des fichiers, des logins et des logs. Ils peuvent également intercepter des données depuis des terminaux, des connexions réseaux, s'ils incluent les logiciels appropriés.

Les Rootkits ne sont pas malveillants par nature. Par exemple, les systèmes d'exploitation et même certaines applications cachent des fichiers sensibles en utilisant des rootkits. Cependant, ils sont principalement utilisés pour camoufler des codes malveillants ou pour cacher la présence d'un intrus sur le système. Lorsqu'ils sont combinés à des codes malveillants, les rootkits sont une menace importante contre l'intégrité et la sécurité d'un système. Ils peuvent analyser le trafic, créer des portes dérobées sur le système, corrompre des fichiers et des logs et éviter leur détection.

Scripts

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

Spam

Message électronique ou envoi de messages souvent répertoriés comme des emails « non sollicités ».

Spyware

Tout type de logiciel qui récupère secrètement les informations des utilisateurs au travers de leur connexion Internet sans les avertir, généralement à des fins publicitaires. Les spywares sont généralement cachés dans des logiciels shareware ou freeware qui peuvent être téléchargés sur Internet. Cependant, la majorité des applications shareware ou freeware ne comportent pas de

spyware. Après son installation, le spyware surveille l'activité de l'utilisateur sur Internet et transmet discrètement des informations à une tierce personne. Les spywares peuvent également récupérer des informations sur les adresses mail, les mots de passe ou même les numéros de cartes de crédit.

Leur point commun avec les Chevaux de Troie est que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une de manière les plus classique pour être victime de spywares est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d'éthique et de respect de la vie privée, les spywares volent aussi les ressources de l'ordinateur de l'utilisateur en utilisant de la bande passante lors de l'envoi d'information au travers de sa connexion Internet. A cause de cette utilisation de la mémoire et des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu'à entraîner des plantages ou provoquer une instabilité globale du système.

Objets menu démarrage

Tous les fichiers placés dans ce dossier s'ouvrent au démarrage. Par exemple, un écran de démarrage, un fichier son pour quand l'ordinateur démarre, un calendrier, des programmes, peuvent être placées dans ce dossier. D'habitude c'est un raccourci vers le fichier qui est mis dans le dossier, et pas le fichier.

Zone de notification

Introduit avec Windows 95, le system tray se situe dans la barre de tâches Windows (à côté de l'horloge) et contient des icônes miniatures pour des accès faciles aux fonctions système: fax, imprimante, modem, volume etc. Double cliquez ou clic droit sur une icône pour voir les options.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés avec divers architectures hardware et diverses plates-formes. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.

Trojan (Cheval de Troie)

Un programme destructif qui prétend être une application normale. Les Trojans ne sont pas des virus et ne se repliquent pas, mais peuvent être tout aussi destructifs. Un des types les plus répandu de Trojans est un logiciel prétendant désinfecter votre PC (mais au lieu de faire cela il l'infecte).

Le terme provient de la fameuse histoire de l'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Trojans, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Mise à jour

Une nouvelle version du logiciel ou d'un produit hardware, destinée à remplacer une ancienne version du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, sinon la mise à jour ne se fait pas.

BitDefender a son propre module de mise à jour permettant à l'utilisateur de vérifier manuellement les mises à jour ou de les programmer automatiquement.

Virus

Programme ou morceau de code qui est chargé dans votre ordinateur sans que vous le sachiez et fonctionne contre votre gré. La plupart des virus peuvent se répliquer. Tous les virus sont créés par des personnes. Un virus simple capable de se copier continuellement est relativement facile à créer. Même un virus simple de ce type est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est capable de se transmettre via un réseau et d'échapper aux systèmes de sécurité.

Définition virus

La "signature" binaire du virus, utilisé par l'antivirus pour la détection et l'élimination du virus.

Ver

Un programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure qu'il se propage. Il ne peut pas s'attacher aux autres programmes.